

Information in the US-CERT Cyber Security Bulletin is a compilation and includes information published by outside sources, so the information should not be considered the result of US-CERT analysis. Software vulnerabilities are categorized in the appropriate section reflecting the operating system on which the vulnerability was reported; however, this does not mean that the vulnerability only affects the operating system reported since this information is obtained from open-source information.

This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to vulnerabilities that appeared in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking **High**. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

Vulnerabilities

- Windows Operating Systems
 - Adaptive Hosting Solutions ProductCart Cross-Site Scripting and SQL Injection Vulnerabilities
 - **ArGoSoft FTP Server 'DELE' Command Remote Buffer Overflow (Updated)**
 - ASP-DEV XM Forum Cross-Site Scripting Vulnerability
 - BakBone NetVault Buffer Overflows Permit Remote Code Execution
 - Bjornar Henden 'Yet Another Forum.net' Input Validation Errors Permits Cross-Site Scripting
 - Comersus Cross-Site Scripting Vulnerability
 - FastStone 4in1 Browser Information Disclosure Vulnerability
 - Iatek SiteEnable SQL Command Injection and Cross-Site Scripting Vulnerabilities
 - Iatek PortalApp SQL Injection and Cross-Site Scripting Vulnerabilities
 - IVT BlueSoleil Directory Traversal Vulnerability
 - Kerio Personal Firewall Access Vulnerability
 - MailEnable Denial of Service Vulnerability
 - MaxWebPortal SQL Injection and Cross-Site Scripting Vulnerabilities
 - Microsoft Jet Database Remote Code Execution Vulnerability
 - Microsoft Windows Explorer and Internet Explorer Denial of Service Vulnerability
 - Microsoft Windows Server 2003 Local Denial of Service Vulnerabilities
 - NetManage RUMBA Profile Handling Multiple Buffer Overflow
 - **Symantec Multiple Products AutoProtect Errors Denial of Service Vulnerability (Updated)**
- UNIX / Linux Operating Systems
 - Andrew Church IRC Services LISTLINKS Information Disclosure
 - BZip2 File Permission Modification
 - **Carnegie Mellon University Cyrus IMAP Server Multiple Remote Buffer Overflows (Updated)**
 - **Dnsmasq Multiple Remote Vulnerabilities (Updated)**
 - FreeBSD Kernel 'sendfile()' Information Disclosure
 - GNU GZip File Permission Modification
 - **GNU Sharutils Multiple Buffer Overflow (Updated)**
 - GNU Sharutils 'Unshar' Insecure Temporary File Creation
 - **GNU Xpdf Buffer Overflow in dolmage() (Updated)**
 - **Grip CDDb Query Buffer Overflow (Updated)**
 - IBM AIX 'RC.BOOT' Insecure Temporary File Creation
 - **ImageMagick Multiple Remote Vulnerabilities (Updated)**
 - **ImageMagick Remote EXIF Parsing Buffer Overflow (Updated)**
 - **LibEXIF Library EXIF Tag Structure Validation (Updated)**
 - **LibTIFF Buffer Overflows (Updated)**
 - Mailreader 'Network.cgi' Arbitrary Code Execution
 - **Multiple Vendors Cyrus IMAPD Multiple Remote Vulnerabilities (Updated)**
 - **Multiple Vendors FreeNX 'XAUTHORITY' Authentication Bypass (Updated)**
 - **Multiple Vendors ht://Dig Cross-Site Scripting (Updated)**
 - **Linux Kernel Multiple ISO9660 Filesystem Handling Vulnerabilities (Updated)**
 - **Multiple Vendors Sylpheed MIME-Encoded Attachment Name Buffer Overflow (Updated)**
 - **Multiple Vendors Squid Proxy Set-Cookie Headers Information Disclosure (Updated)**
 - **Multiple Vendors cURL / libCURL Kerberos Authentication & 'Curl_input_ntlm()' Remote Buffer Overflows (Updated)**
 - **Multiple Vendors Xpdf PDFTOPS Multiple Integer Overflows (Updated)**
 - **Multiple Vendors IMLib/IMLib2 Multiple BMP Image (Updated)**
 - Multiple Vendors GDK-Pixbuf BMP Image Processing Double Free Remote Denial of Service
 - **Multiple Vendors ImageMagick File Name Handling Remote Format String (Updated)**
 - **Multiple Vendors KAME Racoon Malformed ISAKMP Packet Headers Remote Denial of Service (Updated)**
 - **Multiple Vendors Linux Kernel Bluetooth Signed Buffer Index (Updated)**
 - Multiple Vendors Linux Kernel Serial Driver Mouse And Keyboard Event Injection
 - Multiple Vendors Linux Kernel TmpFS Driver Local Denial of Service

- [Multiple Vendors Linux Kernel Futex Denial of Service](#)
- [Multiple Vendors Linux Kernel Netfilter Memory Leak Denial of Service \(Updated\)](#)
- [Multiple Vendors Linux Kernel Local Denial of Service \(Updated\)](#)
- [Multiple Vendors Linux Kernel Multiple Vulnerabilities \(Updated\)](#)
- [Multiple Vendors Linux Kernel EXT2 File System Information Leak \(Updated\)](#)
- [Multiple Vendors Linux Kernel Asynchronous Input/Output Local Denial Of Service](#)
- [Multiple Vendors Gaim 'Gaim_Markup_Strip_HTML\(\)' Function Remote Denial of Service & IRC Protocol Plug-in Arbitrary Code Execution](#)
- [Multiple Vendors Gaim Jabber File Request Remote Denial of Service](#)
- [Multiple Vendors Samba smbd Security Descriptor \(Updated\)](#)
- [Multiple Vendors LibXPM Bitmap_unit Integer Overflow \(Updated\)](#)
- [OpenBSD Remote Denial of Service](#)
- [PAGFileDB SQL Injection & Cross-Site Scripting](#)
- [phpMyAdmin 'convcharset' Cross-Site Scripting](#)
- [Remstats Local Insecure Temporary File & Remote Code Execution](#)
- [SCO OpenServer NWPrint Command Buffer Overflow](#)
- [YepYep MTFTPD Format String & Buffer Overflow](#)
- [Multiple Operating Systems](#)
 - [AltraSoft EPay Pro Remote File Include & Cross-Site Scripting](#)
 - [Bay Technical Associates RPC3 Telnet Daemon Authentication Bypass](#)
 - [Cisco VPN 3000 Concentrator Remote Denial of Service](#)
 - [Cisco IOS Malformed IKE Packet Remote Denial of Service \(Updated\)](#)
 - [Early Impact ProductCart Multiple Input Validation](#)
 - [PHPNuke Multiple Module Cross-Site Scripting](#)
 - [Horde Application Page Title Cross-Site Scripting](#)
 - [InterAKT Online MX Kart Multiple SQL Injection](#)
 - [Lighthouse Development Squirrelcart SQL Injection](#)
 - [Logics Software LOG-FT Information Disclosure](#)
 - [Star Wars Jedi Knight: Jedi Academy Buffer Overflow](#)
 - [Mozilla Suite/Firefox JavaScript Lambda Information Disclosure](#)
 - [Mozilla Suite/ Firefox/ Thunderbird GIF Image Processing Remote Buffer Overflow \(Updated\)](#)
 - [Multiple Vendors Quake 3 Engine Message Denial of Service](#)
 - [Multiple Vendors Telnet Client 'slc add_reply\(\)' & 'env_opt add\(\)' Buffer Overflows \(Updated\)](#)
 - [MySQL CREATE FUNCTION Remote Code Execution Vulnerability \(Updated\)](#)
 - [MySQL Escalated Privilege Vulnerabilities \(Updated\)](#)
 - [MySQL udf_init\(\) Path Validation Vulnerability \(Updated\)](#)
 - [PHP 'getimagesize\(\)' Multiple Denials of Service](#)
 - [ProfitCode Software PayProCart Directory Traversal & Cross-Site Scripting](#)
 - [Samsung ADSL Router Information Disclosure](#)
 - [SonicWALL SOHO Web Interface Multiple Remote Input Validation](#)
 - [Stalker Software CommuniGate Pro LIST Denial of Service](#)
 - [Toshiba ACPI BIOS Denial of Service](#)

[Recent Exploit Scripts/Techniques](#)

[Trends](#)

[Viruses/Trojans](#)

Vulnerabilities

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the [Multiple Operating Systems](#) section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Adaptive Hosting Solutions ProductCart 2.7	Multiple vulnerabilities have been reported that could let remote malicious users conduct Cross-Site Scripting and SQL injection attacks. This is due to improper input validation in 'advSearch_h.asp,' 'NewCust.asp,' 'storelocator_submit.asp,' 'techErr.asp,' and 'advSearch_h.asp.' No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Adaptive Hosting Solutions ProductCart Cross-Site Scripting and SQL Injection Vulnerabilities	High	Secunia SA14833, April 5, 2005
ArGo Software Design FTP Server 1.4.2 .8	A buffer overflow vulnerability exists in the 'DELE' command, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. No workaround or patch available at time of publishing. An exploit script has been published.	ArGoSoft FTP Server 'DELE' Command Remote Buffer Overflow CAN-2005-0696	Low/ High (High if arbitrary code can be executed)	Security Focus, 12755, March 8, 2005 PacketStorm, April 4, 2005
ASP-DEv XM Forum RC3	A vulnerability has been reported that could let a remote malicious user conduct Cross-Site Scripting attacks. This is because of an input validation error in the 'posts.asp' script. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	ASP-DEv XM Forum Cross-Site Scripting Vulnerability	High	Hackers Center Security Group, Zinho's Security Advisory, March 30, 2005
BakBone NetVault 7.3 and prior versions	Two vulnerabilities have been reported that could let a local or remote malicious user execute arbitrary code on the target system. This is due to a vulnerability when processing the 'configure.cfg' file. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	BakBone NetVault Buffer Overflows Permit Remote Code Execution	High	Security Focus 12967, April 1, 2005
Bjørnar Henden 'Yet Another Forum.net' 0.9.9	An input validation vulnerability has been reported that could let a remote malicious user conduct Cross-Site Scripting attacks. The 'name,' 'location,' and 'subject' fields are not properly validated. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Bjørnar Henden 'Yet Another Forum.net' Input Validation Errors Permits Cross-Site Scripting CAN-2005-0982	High	Security Tracker Alert ID: 1013632, April 4, 2005
Comersus Open Technologies Comersus 6	A input validation vulnerability has been reported in the 'username' field could let a remote malicious user conduct Cross-Site Scripting attacks. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Comersus Cross-Site Scripting Vulnerability	High	Hackers Center Security Group, Zinho's Security Advisory, April 3, 2005
FastStone Soft FastStone 4in1 1.2	A directory traversal vulnerability has been reported that could let a remote malicious user view files on the target system. This is due to an input validation error. Update to version 1.3: http://www.faststone.org/FSBrowserDetail.htm A Proof of Concept exploit has been published.	FastStone 4in1 Browser Information Disclosure Vulnerability CAN-2005-0950	Medium	Secunia SA14743, March 30, 2005
latek SiteEnable	Multiple input validation vulnerabilities have been reported that could let a remote malicious user issue SQL commands or conduct Cross-Site Scripting attacks. The 'content.asp' script does not properly validate user-supplied input in the 'sortby' parameter; the 'contenttype' parameter is not properly validated; the title and description fields in the 'Submit a Quote' page are not properly validated. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	latek SiteEnable SQL Command Injection and Cross-Site Scripting Vulnerabilities	High	Hackers Center Security Group, Zinho's Security Advisory, April 1, 2005
latek PortalApp	An input validation vulnerability has been reported that could let a remote malicious user inject SQL commands and conduct Cross-Site Scripting attacks. The 'ad_click.asp' script does not correctly verify input to the 'banner_id' parameter. Also, the 'content.asp' script does not filter HTML code from user-supplied input in the 'contenttype' and 'keywords' parameters. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	latek PortalApp SQL Injection and Cross-Site Scripting Vulnerabilities CAN-2005-0948 CAN-2005-0949	High	Security Tracker Alert ID: 1013591, March 29, 2005

IVT Corporation BlueSoleil Version PTP-1.4.9-Win2k/XP-04.08.27 with Stack Version 04.03.11.20040827	A vulnerability has been reported that could let a remote malicious user traverse the directory when sending files to the target device. This is because a user can exploit the Object Push Service. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	IVT BlueSoleil Directory Traversal Vulnerability CAN-2005-0978	Medium	Security Focus 12961, April 1, 2005
Kerio Technologies Kerio Personal Firewall 4.1.2 and prior	A vulnerability has been reported that could let local malicious users bypass the firewall rules by impersonating another process that is allowed to access the Internet. Update to version 4.1.3: http://www.kerio.com/kpf_download.html Currently we are not aware of any exploits for this vulnerability.	Kerio Personal Firewall Access Vulnerability CAN-2005-0964	Medium	Kerio Security Advisory KSEC-2005-03-30-01, March 30, 2004
MailEnable MailEnable Professional 1.54; Enterprise 1.04	A vulnerability was reported in the IMAP and SMTP services that could let a remote malicious user cause a Denial of Service in the SMTP service to crash. The IMAP impact was not specified. An update is available at: http://www.mailenable.com/hotfix/MEIMSM-HF050404.zip An exploit script has been published.	MailEnable Denial of Service Vulnerability	Low	Security Focus 12994 and 12995, April 5, 2005
MaxWebPortal.com MaxWebPortal 1.33	Some input validation vulnerabilities have been reported that could let a remote malicious user issue SQL commands and conduct Cross-Site Scripting attacks. This is because the EVENT_ID parameter in the Update_Events function in 'events_functions.asp' is not properly validated. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	MaxWebPortal SQL Injection and Cross-Site Scripting Vulnerabilities	High	Security Tracker Alert ID: 1013617, March 31, 2005
Microsoft Jet Database msjet40.dll library version 4.00.8618.0	A vulnerability was reported that could let a remote malicious user cause arbitrary code to be executed. This is because the 'msjet40.dll' component does not properly validate user-supplied input when parsing database files. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Microsoft Jet Database Remote Code Execution Vulnerability CAN-2005-0945	High	Hexview Advisory, ID: HEXVIEW* 2005*03*31*1
Microsoft Windows Explorer and Internet Explorer in Windows 2000 SP1	A vulnerability has been reported that could let remote malicious users cause a Denial of Service via a malformed Windows Metafile (WMF) file. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Microsoft Windows Explorer and Internet Explorer Denial of Service Vulnerability CAN-2005-0954	Low	Bugtraq: 20050331, March 31, 2005
Microsoft Microsoft Windows Server 2003 Datacenter Edition, Enterprise Edition, Standard Edition, Web Edition	Multiple vulnerabilities have been reported that could let a local malicious users cause a Denial of Service. One vulnerability is caused due to an error when the SMB redirector receives a browser announcement frame and tries to run code that is paged out. Another vulnerability is caused due to an error in the printer driver. Update to Service Pack 1 for Windows Server 2003: Windows Server 2003 SP1 (32-bit): http://www.microsoft.com/downloads/details.aspx?FamilyId=22CFC239-337C-4D81-8354-72593B1C1F43 Windows Server 2003 SP1 (Itanium): http://www.microsoft.com/downloads/details.aspx?FamilyId=890C5C44-815C-45BD-8B08-4FE901BB8FDF Currently we are not aware of any exploits for these vulnerabilities.	Microsoft Windows Server 2003 Local Denial of Service Vulnerabilities	Low	Secunia SA14808, April 5, 2005
NetManage RUMBA 7.3	Multiple buffer overflow vulnerabilities have been reported when RTO and WPA profiles are loaded, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	RUMBA Profile Handling Multiple Buffer Overflow CAN-2005-0979	Low/ High (High if arbitrary code can be executed)	Security Focus, 12965, April 1, 2005
Symantec Norton System Works 2004 and 2005, Norton Internet Security 2004 and 2005, Norton AntiVirus 2004 and 2005	Two vulnerabilities were reported in the AutoProtect feature that could let a malicious user create a file or modify a filename to cause a Denial of Service. A user can create a special file of a specific file type that when scanned by the AutoProtect feature will cause a Denial of Service. Also, if a certain type of shared file has its filename modified, the SmartScan analysis of the filename modification may cause a Denial of Service. A fix is available via LiveUpdate. Currently we are not aware of any exploits for these vulnerabilities.	Symantec Multiple Products AutoProtect Errors Denial of Service Vulnerability CAN-2005-0922 CAN-2005-0923	Low	Symantec Advisory, SYM05-006 March 28, 2005 US-CERT VU#146020 US-CERT VU#713620

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Andrew Church IRC Services prior to 5.0.50	A vulnerability has been reported in NickServ LISTLINKS, which could let a remote malicious user obtain sensitive information. Update available at: http://www.ircservices.esper.net/download.html Currently, we are not aware of any exploits for this vulnerability.	IRC Services LISTLINKS Information Disclosure	Medium	Security Tracker Alert, 1013622, April 1, 2005
bzip2 bzip2 1.0.2 & prior	A vulnerability has been reported when an archive is extracted into a world or group writeable directory, which could let a malicious user modify file permissions of target files. No workaround or patch available at time of publishing. There is no exploit code required.	BZip2 File Permission Modification CAN-2005-0953	Medium	Security Focus, 12954, March 31, 2005
Carnegie Mellon University Cyrus IMAP Server 2.x	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in mailbox handling due to an off-by-one boundary error, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists in the imapd annotate extension due to an off-by-one boundary error, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists in 'fetchnews,' which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exist because remote administrative users can exploit the backend; and a buffer overflow vulnerability exists in imapd due to a boundary error, which could let a remote malicious user execute arbitrary code. Update available at: http://ftp.andrew.cmu.edu/pub/cyrus/cyrus-imapd-2.2.11.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200502-29.xml SUSE: ftp://ftp.SUSE.com/pub/SUSE Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/c/cyrus21-imapd/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Conectiva: ftp://atualizacoes.conectiva.com.br/ ALT Linux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html OpenPKG: ftp://ftp.openpkg.org/release/ Currently we are not aware of any exploits for these vulnerabilities.	Cyrus IMAP Server Multiple Remote Buffer Overflows CAN-2005-0546	High	Secunia Advisory, SA14383, February 24, 2005 Gentoo Linux Security Advisory, GLSA 200502-29, February 23, 2005 SUSE Security Announcement, SUSE-SA:2005:009, February 24, 2005 Ubuntu Security Notice USN-87-1, February 28, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:051, March 4, 2005 Conectiva Linux Security Announcement, CLA-2005:937, March 17, 2005 ALTLinux Security Advisory, March 29, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.005, April 5, 2005
Dnsmasq Dnsmasq 2.0-2.20	Multiple vulnerabilities have been reported: a buffer overflow vulnerability has been reported due to an off-by-one error when reading the DHCP lease file, which could let a remote malicious user cause a Denial of Service; and a vulnerability has been reported when receiving DNS replies due to insufficient validation, which could let a remote malicious user poison the DNS cache. Upgrades available at: http://www.thekelleys.org.uk/dnsmasq/dnsmasq-2.21.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200504-03.xml Currently we are not aware of any exploits for these vulnerabilities.	Dnsmasq Multiple Remote Vulnerabilities CAN-2005-0876 CAN-2005-0877	Low/ Medium (Medium if the DNS cache can be poisoned)	Security Focus, 12897, March 25, 2005 Gentoo Linux Security Advisory, GLSA 200504-03, April 4, 2005

FreeBSD FreeBSD 5.4 & prior	<p>A vulnerability has been reported in the 'sendfile()' system call due to a failure to secure sensitive memory before distributing it over the network, which could let a malicious user obtain sensitive information.</p> <p>Patches available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:02/</p> <p>There is no exploit code required.</p>	FreeBSD Kernel 'sendfile()' Information Disclosure CAN-2005-0708	Medium	FreeBSD Security Advisory, FreeBSD-SA-05:02, April 5, 2005
GNU gzip 1.2.4, 1.3.3	<p>A vulnerability has been reported when an archive is extracted into a world or group writeable directory, which could let a malicious user modify file permissions.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required.</p>	GNU GZip File Permission Modification	Medium	Security Focus, 12996, April 5, 2005
GNU sharutils 4.2, 4.2.1	<p>Multiple buffer overflow vulnerabilities exists due to a failure to verify the length of user-supplied strings prior to copying them into finite process buffers, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200410-01.xml</p> <p>FedoraLegacy: http://download.fedoralegacy.org/fedora/</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/sharutils/</p> <p>Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/</p> <p>We are not aware of any exploits for this vulnerability.</p>	GNU Sharutils Multiple Buffer Overflow CAN-2004-1773	Low/ High (High if arbitrary code can be executed)	<p>Gentoo Linux Security Advisory, GLSA 200410-01, October 1, 2004</p> <p>Fedora Legacy Update Advisory, FLSA:2155, March 24, 2005</p> <p>Ubuntu Security Notice, USN-102-1 March 29, 2005</p> <p>Fedora Update Notifications, FEDORA-2005-280 & 281, April 1, 2005</p>
GNU sharutils 4.2, 4.2.1	<p>A vulnerability has been reported in the 'unshar' utility due to the insecure creation of temporary files, which could let a malicious user create/overwrite arbitrary files.</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/sharutils/</p> <p>There is no exploit code required.</p>	GNU Sharutils 'Unshar' Insecure Temporary File Creation	Medium	Ubuntu Security Notice, USN-104-1, April 4, 2005
GNU Xpdf prior to 3.00pl2	<p>A buffer overflow vulnerability exists that could allow a remote user to execute arbitrary code on the target user's system. A remote user can create a specially crafted PDF file that, when viewed by the target user, will trigger an overflow and execute arbitrary code with the privileges of the target user.</p> <p>A fixed version (3.00pl2) is available at: http://www.foolabs.com/xpdf/download.html</p> <p>A patch is available: ftp://ftp.foolabs.com/pub/xpdf/xpdf-3.00pl2.patch</p> <p>KDE: http://www.kde.org/info/security/advisory-20041223-1.txt</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200412-24.xml</p> <p>Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/</p> <p>Mandrakesoft (update for koffice): http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:165</p> <p>Mandrakesoft (update for kdeggraphics): http://www.mandrakesoft.com/security/advisories?name=</p>	GNU Xpdf Buffer Overflow in dolImage() CAN-2004-1125	High	<p>iDEFENSE Security Advisory 12.21.04</p> <p>KDE Security Advisory, December 23, 2004</p> <p>Mandrakesoft, MDKSA-2004:161,162,163,165, 166, December 29, 2004</p> <p>Fedora Update Notification, FEDORA-2004-585, January 6, 2005</p> <p>Gentoo Linux Security Advisory, GLSA 200501-13, January 10, 2005</p> <p>Conectiva Linux Security Announcement, CLA-2005:921, January 25, 2005</p> <p>SUSE Security Summary Report, SUSE-SR:2005:002, January 26, 2005</p> <p>Avaya Security Advisory, ASA-2005-027, January 25, 2005</p> <p>SUSE Security Summary Report,</p>

[MDKSA-2004:163](#)

Mandrakesoft (update for gpdf):
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:162>

Mandrakesoft (update for xpdf):
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:161>

Mandrakesoft (update for tetex):
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:166>

Debian:
<http://www.debian.org/security/2004/dsa-619>

Fedora (update for tetex):
<http://download.fedora.redhat.com/pub/fedora/linux/core/updates/>

Fedora:
<http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/>

Gentoo:
<http://security.gentoo.org/glsa/glsa-200501-13.xml>

TurboLinux:
<ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/>

SGI:
http://support.sgi.com/browse/request/linux_patches_by_os

Conectiva:
<ftp://atualizacoes.conectiva.com.br/>

SuSE:
<ftp://ftp.suse.com/pub/suse/>

FedoraLegacy:
<http://download.fedoralegacy.org/fedora/1/updates/>

FedoraLegacy:
<http://download.fedoralegacy.org/redhat/>

SUSE:
<ftp://ftp.SUSE.com/pub/SUSE>

RedHat:
<http://rhn.redhat.com/errata/RHSA-2005-026.html>

RedHat:
<http://rhn.redhat.com/errata/RHSA-2005-354.html>

Currently we are not aware of any exploits for this vulnerability.

SUSE-SR:2005:003,
February 4, 2005

SUSE Security Summary
Report,
SUSE-SR:2005:003,
February 4, 2005

Fedora Legacy
Update Advisory,
FLSA:2353,
February 10, 2005

Fedora Legacy

Update Advisory,
FLSA:2127,
March 2, 2005

SUSE Security
Announcement,
SUSE-SA:2005
:015, March 14, 2005

RedHat Security Advisory,
RHSA-2005:026-15,
March 16, 2005

SuSE Security Summary
Report,
SUSE-SR:2005:008,
March 18, 2005

**RedHat Security
Advisory,
RHSA-2005:354-03,
April 1, 2005**

<p>Grip</p> <p>Grip 3.1.2, 3.2 .0</p>	<p>A buffer overflow vulnerability has been reported in the CDDB protocol due to a boundary error, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code.</p> <p>Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200503-21.xml</p> <p>RedHat: http://rhn.redhat.com/errata/RHSA-2005-304.html</p> <p>Mandrake: http://www.mandrakesecure.net/en/ftp.php</p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>Grip CDDB Query Buffer Overflow</p> <p>CAN-2005-0706</p>	<p>Low/ High</p> <p>(High if arbitrary code can be executed)</p>	<p>Fedora Update Notifications, FEDORA-2005-202 & 203, March 9, 2005</p> <p>Gentoo Linux Security Advisory, GLSA 200503-21, March 17, 2005</p> <p>RedHat Security Advisory, RHSA-2005:304-08, March 28, 2005</p> <p>Mandrakelinux Security Update Advisory, MDKSA-2005:066, April 3, 2005</p>
<p>IBM</p> <p>AIX 5.1 L, 5.1, 5.2 L, 5.2, 5.3 L, 5.3</p>	<p>A vulnerability has been reported in the '/SBIN/RC.BOOT' script due to the insecure creation of temporary files, which could let a malicious user corrupt arbitrary files with superuser privileges.</p> <p>Updates available at: http://www-912.ibm.com/eserver/support/fixes/</p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>IBM AIX 'RC.BOOT' Insecure Temporary File Creation</p>	<p>High</p>	<p>Security Focus, 12992, April 4, 2005</p>
<p>ImageMagick</p> <p>ImageMagick 5.3.3, 5.3.8, 5.4.3, 5.4.4 .5, 5.4.7, 5.4.8 .2-1.1.0 , 5.4.8, 5.5.3 .2-1.2.0, 5.5.4, 5.5.6 .0-20030409, 5.5.6, 5.5.7, 6.0, 6.0.1</p>	<p>Several vulnerabilities have been reported: a remote Denial of Service vulnerability has been reported in the decoder due to a failure to handle malformed TIFF tags; a remote Denial of Service vulnerability has been reported due to a failure to handle malformed TIFF images; a remote Denial of Service vulnerability has been reported due to a failure to handle malformed PSD files; and a buffer overflow vulnerability has been reported in the SGI parser, which could let a remote malicious user execute arbitrary code.</p> <p>Upgrades available at: http://www.imagemagick.org/script/download.php?</p> <p>SuSE: ftp://ftp.suse.com/pub/suse</p> <p>RedHat: http://rhn.redhat.com/errata/RHSA-2005-070.html</p> <p>Debian: http://security.debian.org/pool/updates/main/i/imagemagick/</p> <p>Mandrake: http://www.mandrakesecure.net/en/ftp.php</p> <p>Currently we are not aware of any exploits for these vulnerabilities.</p>	<p>ImageMagick Multiple Remote Vulnerabilities</p> <p>CAN-2005-0759 CAN-2005-0760 CAN-2005-0761 CAN-2005-0762</p>	<p>Low/ High</p> <p>(High if arbitrary code can be executed)</p>	<p>Security Tracker Alert, 1013550, March 24, 2005</p> <p>Debian Security Advisory, DSA 702-1, April 1, 2005</p> <p>Mandrakelinux Security Update Advisory, MDKSA-2005:065, April 3, 2005</p>
<p>ImageMagick</p> <p>ImageMagick 5.3.3, 5.4.3, 5.4.4.5, 5.4.7, 5.4.8 .2-1.1.0, 5.4.8, 5.5.3 .2-1.2.0, 5.5.6 .0-20030409, 5.5.7, 6.0, 6.0.1, 6.0.3-6.0.8</p>	<p>A buffer overflow vulnerability exists in the 'EXIF' parsing routine due to a boundary error, which could let a remote malicious user execute arbitrary code.</p> <p>Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=24099</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/i/imagemagick/</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200411-11.xml</p> <p>Debian: http://security.debian.org/pool/updates/main/i/imagemagick/</p> <p>SUSE: ftp://ftp.SUSE.com/pub/SUSE/i386/update/</p> <p>Mandrakesoft: http://www.mandrakesoft.com/</p>	<p>ImageMagick Remote EXIF Parsing Buffer Overflow</p> <p>CAN-2004-0827 CAN-2004-0981</p>	<p>High</p>	<p>Security Tracker Alert ID, 1011946, October 26, 2004</p> <p>Gentoo Linux Security Advisory, GLSA 200411-11:01, November 6, 2004</p> <p>Debian Security Advisory DSA 593-1, November 16, 2004</p> <p>SUSE Security Announcement, SUSE-SA:2004:041, November 17, 2004</p> <p>SUSE Security Summary Report, SUSE-SR:2004:001, November 24, 2004</p> <p>Mandrakesoft Security Advisory, MDKSA-2004:143,</p>

	security/advisories?name=MDKSA-2004:143 (Red Hat has re-issued it's update.) http://rhn.redhat.com/errata/RHSA-2004-480.html TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Currently we are not aware of any exploits for this vulnerability.			December 6, 2004 Red Hat Security Advisory, RHSA-2004:636-03, December 8, 2004 Turbolinux Security Advisory, TLSA-2005-7, January 26, 2005 Fedora Update Notification, FEDORA-2005-221, March 15, 2005 Fedora Update Notifications, FEDORA-2005-234 & 235, March 30, 2005
libexif libexif 0.6.9, 0.6.11	A vulnerability exists in the 'EXIF' library due to insufficient validation of 'EXIF' tag structure, which could let a remote malicious user execute arbitrary code. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/libe/libexif/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200503-17.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-300.html Mandrake: http://www.mandrakesecure.net/en/ftp.php Currently we are not aware of any exploits for this vulnerability.	LibEXIF Library EXIF Tag Structure Validation CAN-2005-0664	High	Ubuntu Security Notice USN-91-1, March 7, 2005 Fedora Update Notifications, FEDORA-2005-199 & 200, March 8, 2005 Gentoo Linux Security Advisory, GLSA 200503-17, March 12, 2005 RedHat Security Advisory, RHSA-2005:300-08, March 21, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:064, March 31, 2005
libtiff.org LibTIFF 3.6.1 Avaya MN100 (All versions), Avaya Intuity LX (version 1.1-5.x), Avaya Modular Messaging MSS (All versions)	Several buffer overflow vulnerabilities exist: a vulnerability exists because a specially crafted image file can be created, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; a remote Denial of Service vulnerability exists in 'libtiff/tif_dirread.c' due to a division by zero error; and a vulnerability exists in the 'tif_next.c', 'tif_thunder.c', and 'tif_luv.c' RLE decoding routines, which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/t/tiff/ Gentoo: http://security.gentoo.org/glsa/glsa-200410-11.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ OpenPKG: ftp://ftp.openpkg.org/release/ Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Mandrake: http://www.mandrakesecure.net/en/ftp.php SuSE: ftp://ftp.suse.com/pub/suse/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-577.html Slackware: ftp://ftp.slackware.com/pub/slackware/ Conectiva:	LibTIFF Buffer Overflows CAN-2004-0803 CAN-2004-0804 CAN-2004-0886	Low/ High (High if arbitrary code can be execute)	Gentoo Linux Security Advisory, GLSA 200410-11, October 13, 2004 Fedora Update Notification, FEDORA-2004-334, October 14, 2004 OpenPKG Security Advisory, OpenPKG-SA-2004.043, October 14, 2004 Debian Security Advisory, DSA 567-1, October 15, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0054, October 15, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:109 & MDKSA-2004:111, October 20 & 21, 2004 SuSE Security Announcement, SUSE-SA:2004:038, October 22, 2004 RedHat Security Advisory, RHSA-2004:577-16, October 22, 2004

	ftp://atualizacoes.conectiva.com.br/ KDE: Update to version 3.3.2: http://kde.org/download/ Apple Mac OS X: http://www.apple.com/swupdates/ Gentoo: KDE kfax: http://www.gentoo.org/security/en/glsa/glsa-200412-17.xml Avaya: No solution but workarounds available at: http://support.avaya.com/elmodocs2/security/ASA-2005-002_RHSA-2004-577.pdf TurboLinux: http://www.turbolinux.com/update/ Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: http://rhn.redhat.com/errata/RHSA-2005-354.html Proofs of Concept exploits have been published.			Slackware Security Advisory, SSA:2004-305-02, November 1, 2004 Conectiva Linux Security Announcement, CLA-2004:888, November 8, 2004 US-CERT Vulnerability Notes VU#687568 & VU#948752, December 1, 2004 Gentoo Linux Security Advisory, GLSA 200412-02, December 6, 2004 KDE Security Advisory, December 9, 2004 Apple Security Update SA-2004-12-02 Gentoo Security Advisory, GLSA 200412-17 / kfax, December 19, 2004 Avaya Advisory ASA-2005-002, January 5, 2005 Conectiva Linux Security Announcement, CLA-2005:914, January 6, 2005 Turbolinux Security Announcement, January 20, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:052, March 4, 2005 RedHat Security Advisory, RHSA-2005:354-03, April 1, 2005
Mailreader.com Mailreader.com 2.3.29	A vulnerability has been reported in 'network.cgi' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML code. Debian: http://security.debian.org/pool/updates/main/m/mailreader/ There is no exploit code required.	Mailreader 'Network.cgi' Arbitrary Code Execution CAN-2005-0386	High	Debian Security Advisory DSA 700-1, March 30, 2005
Multiple Vendors Carnegie Mellon University Cyrus IMAP Server 2.1.7, 2.1.9, 2.1.10, 2.1.16, 2.2.0 ALPHA, 2.2.1 BETA, 2.2.2 BETA, 2.2.3-2.2.8; Trustix Secure Enterprise Linux 2.0, Secure Linux 2.0-2.2; Ubuntu Linux 4.1 ppc, 4.1 ia64, 4.1 ia32	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in the 'PROXY' and 'LOGIN' commands if the 'IMAPMAGICPLUS' option is enabled, which could let a remote malicious user execute arbitrary code; an input validation vulnerability exists in the argument parser for the 'PARTIAL' command, which could let a remote malicious user execute arbitrary code; an input validation vulnerability exists in the argument handler for the 'FETCH' command, which could let a remote malicious user execute arbitrary code; and a vulnerability exists in the handler for the 'APPEND' command, which could let a remote malicious user execute arbitrary code. Carnegie Mellon University: ftp://ftp.andrew.cmu.edu/pub/cyrus/ Debian: http://security.debian.org/pool/updates/main/c/cyrus-imapd/ Gentoo: http://security.gentoo.org/	Cyrus IMAPD Multiple Remote Vulnerabilities CAN-2004-1011 CAN-2004-1012 CAN-2004-1013	High	Securiteam, November 23, 2004 Debian Security Advisory, DSA 597-1, November 25, 2004 Gentoo Linux Security Advisory, GLSA 200411-34, November 25, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:139, November 26, 2004 Trustix Secure Linux Advisory, TSL-2004-0063. November 29, 2004 OpenPKG Security

	<p>qlsa/qlsa-200411-34.xml</p> <p>Mandrake: http://www.mandrakesecure.net/en/ftp.php</p> <p>Trustix: http://http.trustix.org/pub/trustix/updates/</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/c/cyrus21-imapd/</p> <p>Conectiva: ftp://atualizacoes.conectiva.com.br/</p> <p>Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/</p> <p>OpenPKG: ftp://ftp.openpkg.org/release/</p> <p>SUSE: ftp://ftp.SUSE.com/pub/SUSE/</p> <p>Apple: http://www.apple.com/support/downloads/securityupdate2005003client.html</p> <p>An exploit script has been published.</p>			<p>Advisory, OpenPKG-SA-2004.051, November 29, 2004</p> <p>Conectiva Linux Security Announcement, CLA-2004:904, December 1, 2004</p> <p>Fedora Update Notifications, FEDORA-2004-487 & 489, December 1, 2004</p> <p>SUSE Security Announcement, SUSE-SA:2004:043, December 3, 2004</p> <p>Apple Security Update, APPLE-SA-2005-03-21, March 21, 2005</p> <p>PacketStorm, March 30, 2005</p>
<p>Multiple Vendors</p> <p>FreeNX 0.2 -0-0.2 -3, 0.2.4-0.2.7</p>	<p>A vulnerability exists in the 'XAUTHORITY' environment variable, which could let a malicious user bypass authentication.</p> <p>Update available at: http://debian.tu-bs.de/knoppix/nx/freenx-0.2.8.tar.gz</p> <p>SuSE: ftp://ftp.suse.com/pub/suse/</p> <p>Upgrade available at: http://debian.tu-bs.de/knoppix/nx/freenx-0.2.8.tar.gz</p> <p>There is no exploit code required.</p>	<p>FreeNX 'XAUTHORITY' Authentication Bypass</p> <p>CAN-2005-0579</p>	Medium	<p>SUSE Security Summary Report, ID: SUSE-SR:2005:006, February 25, 2005</p> <p>Security, 12663, April 1, 2005</p>
<p>Multiple Vendors</p> <p>ht//Dig Group ht://Dig 3.1.5 -8, 3.1.5 -7, 3.1.5, 3.1.6, 3.2 .0, 3.2 0b2-0b6; SuSE Linux 8.0, i386, 8.1, 8.2, 9.0, 9.0 x86_64, 9.1, 9.2</p>	<p>A Cross-Site Scripting vulnerability exists due to insufficient filtering of HTML code from the 'config' parameter, which could let a remote malicious user execute arbitrary HTML and script code.</p> <p>SuSE: ftp://ftp.suse.com/pub/suse/</p> <p>Debian: http://security.debian.org/pool/updates/main/h/htdig/</p> <p>Gentoo: http://security.gentoo.org/qlsa/qlsa-200502-16.xml</p> <p>Mandrake: http://www.mandrakesecure.net/en/ftp.php</p> <p>Proof of Concept exploit has been published.</p>	<p>ht://Dig Cross-Site Scripting</p> <p>CVE Name: CAN-2005-0085</p>	High	<p>SUSE Security Summary Report, SUSE-SR:2005:003, February 4, 2005</p> <p>Debian Security Advisory ,DSA 680-1, February 14, 2005</p> <p>Gentoo Linux Security Advisory, GLSA 200502-16, February 14, 2005</p> <p>Mandrakelinux Security Update Advisory, MDKSA-2005:063, March 31, 2005</p>
<p>Multiple Vendors</p> <p>Linux kernel 2.4 .0-test1-test12, 2.4-2.4.29, 2.6, 2.6-test1-test11, 2.6.1-2.6.11</p>	<p>Multiple vulnerabilities have been reported in the ISO9660 handling routines, which could let a malicious user execute arbitrary code.</p> <p>Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/</p> <p>Currently we are not aware of any exploits for these vulnerabilities.</p>	<p>Linux Kernel Multiple ISO9660 Filesystem Handling Vulnerabilities</p> <p>CAN-2005-0815</p>	High	<p>Security Focus, 12837, March 18, 2005</p> <p>Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005</p> <p>Ubuntu Security Notice, USN-103-1, April 1, 2005</p>

Multiple Vendors RedHat Fedora Core3 & Core 2; Sylpheed Sylpheed 0.8, 0.8.11, 0.9.4-0.9.12, 0.9.99, 1.0.0-1.0.3, 1.9-1.9.4	A buffer overflow vulnerability exists in the handling of email messages that contain attachments with MIME-encoded file names, which could let a remote malicious user execute arbitrary code. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Sylpheed: http://sylpheed.good-day.net/sylpheed/v1.0/sylpheed-1.0.4.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200504-02.xml Currently we are not aware of any exploits for this vulnerability.	Sylpheed MIME-Encoded Attachment Name Buffer Overflow CAN-2005-0926	High	Fedora Update Notifications, FEDORA-2005-263 & 264, March 29, 2005 Gentoo Linux Security Advisory, GLSA 200504-02, April 2, 2005
Multiple Vendors Squid Web Proxy Cache 2.5 .STABLE9, .STABLE8, .STABLE7	A vulnerability exists when using the Netscape Set-Cookie recommendations for handling cookies in caches due to a race condition, which could let a malicious user obtain sensitive information. Patches available at: http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE9-setcookie.patch Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/squid/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ There is no exploit code required.	Squid Proxy Set-Cookie Headers Information Disclosure CAN-2005-0626	Medium	Secunia Advisory, SA14451, March 3, 2005 Ubuntu Security Notice, USN-93-1 March 08, 2005 Fedora Update Notifications, FEDORA-2005-275 & 276, March 30, 2005
Multiple Vendors Daniel Stenberg curl 6.0-6.4, 6.5-6.5.2, 7.1, 7.1.1, 7.2, 7.2.1, 7.3, 7.4, 7.4.1, 7.10.1, 7.10.3-7.10.7, 7.12.1	A buffer overflow vulnerability exists in the Kerberos authentication code in the 'Curl_krb_kauth()' and 'krb4_auth()' functions and in the NT Lan Manager (NTLM) authentication in the 'Curl_input_ntlm()' function, which could let a remote malicious user execute arbitrary code. SUSE: ftp://ftp.SUSE.com/pub/SUSE Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/c/curl/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Updates available at: http://curl.haxx.se/download/curl-7.13.1.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200503-20.xml Conectiva: ftp://atualizacoes.conectiva.com.br/10/ ALT Linux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html RedHat: http://rhn.redhat.com/errata/RHSA-2005-340.html Currently we are not aware of any exploits for these vulnerabilities.	Multiple Vendors cURL / libCURL Kerberos Authentication & 'Curl_input_ntlm()' Remote Buffer Overflows CAN-2005-0490	High	iDEFENSE Security Advisory , February 21, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:048, March 4, 2005 Gentoo Linux Security Advisory, GLSA 200503-20, March 16, 2005 Conectiva Linux Security Announcement, CLA-2005:940, March 21, 2005 ALTLinux Security Advisory, March 29, 2005 RedHat Security Advisory, RHSA-2005:340-09, April 5, 2005
Multiple Vendors Debian Linux 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; Easy Software Products CUPS 1.0.4 -8, 1.0.4, 1.1.1, 1.1.4 -5, 1.1.4 -3, 1.1.4 -2, 1.1.4, 1.1.6, 1.1.7, 1.1.10, 1.1.12-1.1.20; Gentoo Linux;	Several integer overflow vulnerabilities exist in 'pdftops/Catalog.cc' and 'pdftops/XRef.cc,' which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/c/cupsys/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Gentoo:	Multiple Vendors Xpdf PDFTOPS Multiple Integer Overflows CAN-2004-0888 CAN-2004-0889	High	Security Tracker Alert ID, 1011865, October 21, 2004 Conectiva Linux Security Announcement, CLA-2004:886, November 8, 2004 Debian Security Advisory, DSA 599-1, November 25, 2004 SUSE Security Summary

<p>GNOME GPdf 0.112; KDE KDE 3.2-3.2.3, 3.3, 3.3.1, kpdf 3.2; RedHat Fedora Core2; Ubuntu ubuntu 4.1, ppc, ia64, ia32, Xpdf Xpdf 0.90-0.93; 1.0.1, 1.0 0a, 1.0, 2.0 3, 2.0 1, 2.0, 3.0, SUSE Linux - all versions</p>	<p>http://security.gentoo.org/glsa/glsa-200410-20.xml</p> <p>KDE: ftp://ftp.kde.org/pub/kde/security_patches/post-3.3.1-kdegraphics.diff</p> <p>Mandrake: http://www.mandrakesecure.net/en/ftp.php</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/c/cupsys/</p> <p>Conectiva: ftp://atualizacoes.conectiva.com.br/</p> <p>Debian: http://security.debian.org/pool/updates/main/t/tetex-bin/</p> <p>SUSE: Update: ftp://ftp.SUSE.com/pub/SUSE</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200501-31.xml</p> <p>Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/</p> <p>FedoraLegacy: http://download.fedoralegacy.org/fedora/1/updates/</p> <p>RedHat: https://rhn.redhat.com/errata/RHSA-2005-132.html</p> <p>FedoraLegacy: http://download.fedoralegacy.org/redhat/</p> <p>RedHat: http://rhn.redhat.com/errata/RHSA-2005-213.html</p> <p>SGI: ftp://patches.sgi.com/support/free/security/advisories/</p> <p>SUSE: ftp://ftp.suse.com/pub/suse/</p> <p>RedHat: http://rhn.redhat.com/errata/RHSA-2005-354.html</p> <p>Currently we are not aware of any exploits for these vulnerabilities.</p>			<p>Report, SUSE-SR:2004:002, November 30, 2004</p> <p>Gentoo Linux Security Advisory, GLSA 200501-31, January 23, 2005</p> <p>Fedora Update Notifications, FEDORA-2005-122, 123, 133-136, February 8 & 9, 2005</p> <p>Fedora Legacy Update Advisory, FLSA:2353, February 10, 2005</p> <p>Mandrakelinux Security Update Advisories, MDKSA-2005: 041-044, February 18, 2005</p> <p>RedHat Security Advisory, RHSA-2005:132-09, February, 18. 2005</p> <p>Fedora Legacy Update Advisory, FLSA:2127, March 2, 2005</p> <p>Mandrakelinux Security Update Advisory, MDKSA-2005:052, March 4, 2005</p> <p>RedHat Security Advisory, RHSA-2005:213-04, March 4, 2005</p> <p>SGI Security Advisory, 20050204-01-U, March 7, 2005</p> <p>SUSE Security Summary Report, SUSE-SR:2005:008, March 18, 2005</p> <p>RedHat Security Advisory, RHSA-2005:354-03, April 1, 2005</p>
<p>Multiple Vendors</p> <p>Enlightenment Imlib2 1.0-1.0.5, 1.1, 1.1.1; ImageMagick ImageMagick 5.4.3, 5.4.4 .5, 5.4.8 .2-1.1.0 , 5.5.3 .2-1.2.0, 5.5.6 .0- 2003040, 5.5.7,6.0.2; Imlib Imlib 1.9-1.9.14</p>	<p>Multiple buffer overflow vulnerabilities exist in the Imlib/Imlib2 libraries when handling malformed bitmap images, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.</p> <p>Imlib: http://cvs.sourceforge.net/viewcvs.py/enlightenment/e17/</p> <p>ImageMagick: http://www.imagemagick.org/www/download.html</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200409-12.xml</p> <p>Mandrake: http://www.mandrakesecure.net/en/ftp.php</p> <p>Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/</p> <p>Debian: http://security.debian.org/pool/</p>	<p>IMLib/IMLib2 Multiple BMP Image Decoding Buffer Overflows</p> <p>CAN-2004-0817 CAN-2004-0802</p>	<p>Low/ High</p> <p>(High if arbitrary code can be executed)</p>	<p>Security Focus, September 1, 2004</p> <p>Gentoo Linux Security Advisory, GLSA 200409-12, September 8, 2004</p> <p>Mandrakelinux Security Update Advisory, MDKSA-2004:089, September 8, 2004</p> <p>Fedora Update Notifications, FEDORA-2004-300 &301, September 9, 2004</p> <p>Turbolinux Security Advisory, TLSA-2004-27, September 15, 2004</p> <p>RedHat Security Advisory, RHSA-2004:465-08,</p>

	<p>updates/main/i/imagemagick/</p> <p>RedHat: http://rhn.redhat.com/errata/RHSA-2004-465.html</p> <p>SUSE: ftp://ftp.SUSE.com/pub/SUSE/</p> <p>TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/Desktop/</p> <p>Conectiva: ftp://atualizacoes.conectiva.com.br/</p> <p>Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57648-1&searchclause= http://sunsolve.sun.com/search/document.do?assetkey=1-26-57645-1&searchclause=</p> <p>TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/</p> <p>RedHat: http://rhn.redhat.com/errata/RHSA-2004-480.html</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/i/imagemagick/i</p> <p>RedHat: http://rhn.redhat.com/errata/RHSA-2004-636.html</p> <p>SUSE: ftp://ftp.SUSE.com/pub/SUSE/</p> <p>Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/</p> <p>Currently we are not aware of any exploits for these vulnerabilities.</p>			<p>September 15, 2004</p> <p>Debian Security Advisories, DSA 547-1 & 548-1, September 16, 2004</p> <p>Conectiva Linux Security Announcement, CLA-2004:870, September 28, 2004</p> <p>Sun(sm) Alert Notifications, 57645 & 57648, September 20, 2004</p> <p>Turbolinux Security Announcement, October 5, 2004</p> <p>RedHat Security Update, RHSA-2004:480-05, October 20, 2004</p> <p>Ubuntu Security Notice USN-35-1, November 30, 2004</p> <p>RedHat Security Advisory, RHSA-2004:636-03, December 8, 2004</p> <p>SUSE Security Summary Report, SUSE-SR:2005:002, January 26, 2005</p> <p>Fedora Update Notifications, FEDORA-2005-234 & 235, March 30, 2005</p>
<p>Multiple Vendors</p> <p>GNOME GdkPixbuf 0.22</p> <p>GTK GTK+ 2.4.14</p> <p>RedHat Fedora Core3</p> <p>RedHat Fedora Core2</p>	<p>A remote Denial of Service vulnerability has been reported due to a double free error in the BMP loader.</p> <p>Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/</p> <p>RedHat: http://rhn.redhat.com/errata/RHSA-2005-344.html http://rhn.redhat.com/errata/RHSA-2005-343.html</p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>GDK-Pixbuf BMP Image Processing Double Free Remote Denial of Service</p> <p>CAN-2005-0891</p>	<p>Low</p>	<p>Fedora Update Notifications, FEDORA-2005-265, 266, 267 & 268, March 30, 2005</p> <p>RedHat Security Advisories, RHSA-2005:344-03 & RHSA-2005:343-03, April 1 & 4, 2005</p>
<p>Multiple Vendors</p> <p>ImageMagick 5.3.3, 5.4.3, 5.4.4 .5, 5.4.7, 5.4.8 .2-1.1.0, 5.4.8, 5.5.3 .2-1.2.0, 5.5.6 .0-20030409, 5.5.7, 6.0-6.0.8, 6.1-6.1.7, 6.2</p>	<p>A format string vulnerability exists when handling malformed file names, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.</p> <p>Update available at: http://www.imagemagick.org/script/downloads.php</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/i/imagemagick/</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200503-11.xml</p> <p>SUSE: ftp://ftp.suse.com/pub/suse/</p> <p>RedHat: http://rhn.redhat.com/errata/RHSA-2005-320.html</p> <p>Fedora:</p>	<p>ImageMagick File Name Handling Remote Format String</p> <p>CAN-2005-0397</p>	<p>Low/ High</p> <p>(High if arbitrary code can be executed)</p>	<p>Secunia Advisory, SA14466, March 4, 2005</p> <p>Ubuntu Security Notice, USN-90-1, March 3, 2004</p> <p>SUSE Security Announcement, SUSE-SA:2005:017, March 23, 2005</p> <p>RedHat Security Advisory, RHSA-2005:320-10, March 23, 2005</p> <p>Fedora Update Notifications, FEDORA-2005-234 & 235, March 30, 2005</p> <p>Debian Security Advisory,</p>

	http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Debian: http://security.debian.org/pool/updates/main/i/imagemagick/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Currently we are not aware of any exploits for this vulnerability.			DSA 702-1 , April 1, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:065, April 3, 2005
Multiple Vendors IPsec-Tools IPsec-Tools 0.5; KAME Racoon prior to 20050307	A remote Denial of Service vulnerability has been reported when parsing ISAKMP headers. Upgrades available at: http://www.kame.net/snap-users/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-232.html Gentoo: http://security.gentoo.org/glsa/glsa-200503-30.xml ALTLinux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html SUSE: ftp://ftp.SUSE.com/pub/SUSE Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/i/ipsec-tools/ Currently we are not aware of any exploits for this vulnerability.	KAME Racoon Malformed ISAKMP Packet Headers Remote Denial of Service CAN-2005-0398	Low	Fedora Update Notifications, FEDORA-2005-216 & 217, March 14, 2005 RedHat Security Advisory, RHSA-2005:232-10, March 23, 2005 Gentoo Linux Security Advisory, GLSA 200503-33, March 25, 2005 ALTLinux Security Advisory, March 29, 2005 SUSE Security Announcement, SUSE-SA:2005:020, March 31, 2005 Ubuntu Security Notice, USN-107-1, April 05, 2005
Multiple Vendors Linux kernel 2.4-2.4.29, 2.6 .10, 2.6-2.6.11	A vulnerability has been reported in the 'bluez_sock_create()' function when a negative integer value is submitted, which could let a malicious user execute arbitrary code with root privileges. Patches available at: http://www.kernel.org/pub/linux/kernel/v2.4/testing/patch-2.4.30-rc3.bz2 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Trustix: http://http.trustix.org/pub/trustix/updates/ A Proof of Concept exploit script has been published.	Linux Kernel Bluetooth Signed Buffer Index CAN-2005-0750	High	Security Tracker Alert, 1013567, March 27, 2005 SUSE Security Announcement, SUSE-SA:2005:021, April 4, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0011, April 5, 2005 US-CERT VU#685461
Multiple Vendors Linux kernel 2.4-2.4.30, 2.6-2.6.11	A vulnerability has been reported due to insufficient access control of the 'N_MOUSE' line discipline, which could let a malicious user inject mouse and keyboard events into an alternate X session or console. Patches available at: http://www.securityfocus.com/data/vulnerabilities/patches/serport.patch Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/ Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Serial Driver Mouse And Keyboard Event Injection CAN-2005-0839	Medium	Security Focus, 12971, April 1, 2005
Multiple Vendors Linux kernel 2.4-2.4.30, 2.6-2.6.11; Ubuntu Linux 4.1 ppc, ia64, ia32	A Denial of Service vulnerability has been reported in the 'TmpFS' driver due to insufficient sanitization of the 'shm_nopage()' argument. Patch available at: http://www.securityfocus.com/data/vulnerabilities/patches/shmem.patch Ubuntu: http://security.ubuntu.com/ubuntu/	Linux Kernel TmpFS Driver Local Denial of Service CAN-2005-0977	Low	Security Focus, 12970 April 1, 2005

	pool/main//linux-source-2.6.8.1/ Currently we are not aware of any exploits for this vulnerability.			
Multiple Vendors Linux kernel 2.5.0-2.5.69, 2.6-2.6.11	A Denial of Service vulnerability has been reported in 'kernel/futex.c.' No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Futex Denial of Service CAN-2005-0937	Low	Security Tracker Alert, 1013616, March 31, 2005
Multiple Vendors Linux kernel 2.6 .10, Linux kernel 2.6 -test1-test11, 2.6-2.6.8	A Denial of Service vulnerability has been reported in the Netfilter code due to a memory leak. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main//linux-source-2.6.8.1/ SuSE: ftp://ftp.suse.com/pub/suse/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Netfilter Memory Leak Denial of Service CAN-2005-0210	Low	Ubuntu Security Notice, USN-95-1 March 15, 2005 SUSE Security Announcement, SUSE-SA:2005:018, March 24, 2005 Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005 Conectiva Linux Security Announcement, CLA-2005:945, March 31, 2005
Multiple Vendors Linux Kernel 2.6.10, 2.6 -test1-test11, 2.6-2.6.11	A Denial of Service vulnerability has been reported in the 'load_elf_library' function. Patches available at: http://www.kernel.org/pub/linux/kernel/v2.6/patch-2.6.11.6.bz2 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Trustix: http://http.trustix.org/pub/trustix/updates/ Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Local Denial of Service CAN-2005-0749	Low	Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005 Trustix Secure Linux Security Advisory, TLSA-2005-0011, April 5, 2005
Multiple Vendors Linux kernel 2.6.10, 2.6 -test9-CVS, 2.6-test1-test11, 2.6, 2.6.1-2.6.11 ; RedHat Desktop 4.0, Enterprise Linux WS 4, ES 4, AS 4	Multiple vulnerabilities exist: a vulnerability exists in the 'shmctl' function, which could let a malicious user obtain sensitive information; a Denial of Service vulnerability exists in 'nls_ascii.c' due to the use of incorrect table sizes; a race condition vulnerability exists in the 'setsid()' function; and a vulnerability exists in the OUTS instruction on the AMD64 and Intel EM64T architecture, which could let a malicious user obtain elevated privileges. RedHat: https://rhn.redhat.com/errata/RHSA-2005-092.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main//linux-source-2.6.8.1/ Conectiva: ftp://atualizacoes.conectiva.com.br/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ Currently we are not aware of any exploits for these vulnerabilities.	Linux Kernel Multiple Vulnerabilities CAN-2005-0176 CAN-2005-0177 CAN-2005-0178 CAN-2005-0204	Low/ Medium (Low if a DoS)	Ubuntu Security Notice, USN-82-1, February 15, 2005 RedHat Security Advisory, RHSA-2005:092-14, February 18, 2005 SUSE Security Announcement, SUSE-SA:2005:018, March 24, 2005 Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005 Conectiva Linux Security Announcement, CLA-2005:945, March 31, 2005
Multiple Vendors Linux kernel 2.6.10, 2.6, -test1-test 11, 2.6.1- 2.6.11; RedHat Fedora Core2	A vulnerability has been reported in the EXT2 filesystem handling code, which could let malicious user obtain sensitive information. Patches available at: http://www.kernel.org/pub/linux/kernel/v2.6/patch-2.6.11.6.bz2 Fedora: http://download.fedora.redhat.com/	Linux Kernel EXT2 File System Information Leak CAN-2005-0400	Medium	Security Focus, 12932, March 29, 2005 Trustix Secure Linux Security Advisory, TLSA-2005-0011, April 5, 2005

	pub/fedoraproject.org/linux/core/updates/2/ Trustix: http://http.trustix.org/pub/trustix/updates/ Currently we are not aware of any exploits for this vulnerability.			
Multiple Vendors Linux kernel 2.6.8 rc1-rc3, 2.6.8, 2.6.11-rc2-rc4, 2.6.11	A Denial of Service vulnerability has been reported due to an error in the AIO (Asynchronous I/O) support in the "is_hugepage_only_range()" function. No workaround or patch available at time of publishing. Currently, we are not aware of any exploits for this vulnerability.	Linux Kernel Asynchronous Input/Output Local Denial Of Service CAN-2005-0916	Low	Secunia Advisory, SA14718, April 4, 2005
Multiple Vendors RedHat Fedora Core3, Core2; Rob Flynn Gaim 1.2; Ubuntu Linux 4.1 ppc, ia64, ia32	Two vulnerabilities have been reported: a remote Denial of Service vulnerability has been reported due to a buffer overflow in the 'gaim_markup_strip_html()' function; and a vulnerability has been reported in the IRC protocol plug-in due to insufficient sanitization of the 'irc_msg' data, which could let a remote malicious user execute arbitrary code. Update available at: http://gaim.sourceforge.net/downloads.php Fedora: http://download.fedoraproject.org/pub/fedora/linux/core/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gaim/ Currently we are not aware of any exploits for these vulnerabilities.	Gaim 'Gaim_Markup_Strip_HTML()' Function Remote Denial of Service & IRC Protocol Plug-in Arbitrary Code Execution CAN-2005-0965 CAN-2005-0966	Low/ High (High if arbitrary code can be executed)	Fedora Update Notifications, FEDORA-2005-298 & 299, April 5, 2005 Ubuntu Security Notice, USN-106-1 April 05, 2005
Multiple Vendors RedHat Fedora Core3, Core2; Rob Flynn Gaim 1.2	A remote Denial of Service vulnerability has been reported when an unspecified Jabber file transfer request is handled. Upgrade available at: http://gaim.sourceforge.net/downloads.php Fedora: http://download.fedoraproject.org/pub/fedora/linux/core/updates/ There is no exploit code required.	Gaim Jabber File Request Remote Denial of Service	Low	Fedora Update Notifications, FEDORA-2005-298 & 299, April 5, 2005
Multiple Vendors Samba 2.2.9, 3.0.8 and prior	An integer overflow vulnerability in all versions of Samba's smbd 0.8 could allow an remote malicious user to cause controllable heap corruption, leading to execution of arbitrary commands with root privileges. Patches available at: http://www.samba.org/samba/ftp/patches/security/samba-3.0.9-CAN-2004-1154.patch Red Hat: http://rhn.redhat.com/errata/RHSA-2004-670.html Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200412-13.xml Trustix: http://www.trustix.net/errata/2004/0066/ Red Hat (Updated): http://rhn.redhat.com/errata/RHSA-2004-670.html Fedora: http://download.fedoraproject.org/pub/fedora/linux/core/updates/ SUSE: http://www.novell.com/linux/security/advisories/2004_45_samba.html Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:158 Conectiva: ftp://atualizacoes.conectiva.com.br/	Multiple Vendors Samba smbd Security Descriptor CAN-2004-1154	High	iDEFENSE Security Advisory 12.16.04 Red Hat Advisory, RHSA-2004:670-10, December 16, 2004 Gentoo Security Advisory, GLSA 200412-13 / Samba, December 17, 2004 US-CERT, Vulnerability Note VU#226184, December 17, 2004 Trustix Secure Linux Advisory #2004-0066, December 17, 2004 Red Hat, RHSA-2004:670-10, December 16, 2004 SUSE, SUSE-SA:2004:045, December 22, 2004 RedHat Security Advisory, RHSA-2005:020-04, January 5, 2005 Conectiva Linux Security Announcement, CLA-2005:913, January 6, 2005 Turbolinux Security Announcement, February

	<p>RedHat: http://rhn.redhat.com/errata/RHSA-2005-020.html</p> <p>HP: http://software.hp.com</p> <p>TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/</p> <p>SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.17</p> <p>Debian: http://security.debian.org/pool/updates/main/s/samba/</p> <p>Currently we are not aware of any exploits for this vulnerability.</p>			<p>7, 2005</p> <p>HP Security Advisory, HPSBUX01115, February 3, 2005</p> <p>SCO Security Advisory, SCOSA-2005.17, March 7, 2005</p> <p>Debian Security Advisory, DSA 701-1, March 31, 2005</p>
<p>Multiple Vendors</p> <p>X.org X11R6 6.7.0, 6.8, 6.8.1; XFree86 X11R6 3.3, 3.3.2-3.3.6, 4.0, 4.0.1, 4.0.2 -11, 4.0.3, 4.1.0, 4.1 -12, 4.1 -11, 4.2 .0, 4.2.1 Errata, 4.2.1, 4.3.0.2, 4.3.0.1, 4.3.0</p>	<p>An integer overflow vulnerability exists in 'scan.c' due to insufficient sanity checks on on the 'bitmap_unit' value, which could let a remote malicious user execute arbitrary code.</p> <p>Patch available at: https://bugs.freedesktop.org/attachment.cgi?id=1909</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200503-08.xml</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/lesstif1-1/</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200503-15.xml</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/x/xfree86/</p> <p>ALTLinux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html</p> <p>Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/</p> <p>RedHat: http://rhn.redhat.com/errata/RHSA-2005-331.html</p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>LibXPM Bitmap_unit Integer Overflow</p> <p>CAN-2005-0605</p>	<p>High</p>	<p>Security Focus, 12714, March 2, 2005</p> <p>Gentoo Linux Security Advisory, GLSA 200503-08, March 4, 2005</p> <p>Ubuntu Security Notice, USN-92-1 March 07, 2005</p> <p>Gentoo Linux Security Advisory, GLSA 200503-15, March 12, 2005</p> <p>Ubuntu Security Notice, USN-97-1 March 16, 2005</p> <p>ALTLinux Security Advisory, March 29, 2005</p> <p>Fedora Update Notifications, FEDORA-2005 -272 & 273, March 29, 2005</p> <p>RedHat Security Advisory, RHSA-2005: 331-06, March 30, 2005</p>
<p>OpenBSD</p> <p>OpenBSD 3.5, 3.6</p>	<p>Multiple remote Denials of Service vulnerabilities has been reported in 'tcp_input.c' and 'tcp_usrreq.c' when a malicious user submits TCP packets with invalid SACK options.</p> <p>Patches available at: ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.5/common/030_sack.patch ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.6/common/013_sack.patch</p> <p>Currently we are not aware of any exploits for these vulnerabilities.</p>	<p>OpenBSD Remote Denial of Service</p> <p>CAN-2005-0960</p>	<p>Low</p>	<p>Security Tracker Alert, 1013611, March 30, 2005</p>
<p>PHP Arena</p> <p>paFileDB 1.1.3, 2.1.1, 3.0 Beta 3.1, 3.0, 3.1</p>	<p>Two vulnerabilities have been reported: a vulnerability has been reported in 'pafiledb.php' due to insufficient sanitization of the 'sortby' parameter, which could let a remote malicious user inject arbitrary SQL commands; and a Cross-Site Scripting vulnerability has been reported in 'pafiledb.php' due to insufficient sanitization of the 'id' parameter, which could let a remote malicious user execute arbitrary HTML and script code.</p> <p>No workaround or patch available at time of publishing.</p>	<p>PAFileDB SQL Injection & Cross-Site Scripting</p> <p>CAN-2005-0951 CAN-2005-0952</p>	<p>High</p>	<p>Dcrab 's Security Advisory, March 30, 2005</p>

	There is no exploit code required; however, a Proof of Concept exploit has been published.			
phpMyAdmin phpMyAdmin 2.0-2.0.5, 2.1- 2.1.2, 2.2, pre 1&pre2, rc1-rc3, 2.2.2-2.2.6, 2.3.1, 2.3.2, 2.4.0, 2.5.0-2.5.2, 2.5.4-2.5.7, 2.6.0pl1-2.6.0pl3, 2.6.1, pl1&pl3, 2.6.1-rc1	<p>A Cross-Site Scripting vulnerability has been reported in 'index.php' due to insufficient sanitization of the 'convcharset' parameter, which could let a remote malicious user execute arbitrary HTML and script code.</p> <p>Upgrades available at: http://prdownloads.sourceforge.net/phpmyadmin/phpMyAdmin-2.6.2-rc1.tar.gz?download</p> <p>There is no exploit code required; however, a Proof of Concept exploit has been published.</p>	phpMyAdmin 'convcharset' Cross-Site Scripting	High	phpMyAdmin Security Announcement, PMASA-2005-3, April 3, 2005
Remstats Network Analysis Utility 1.0 a4-1.0.13 a	<p>Several vulnerabilities have been reported: a vulnerability has been reported due to the creation of insecure files, which could let a remote malicious user create/overwrite arbitrary files; and a vulnerability has been reported due to insufficient sanitization of user-supplied input before carrying out critical functionality, which could let a remote malicious user execute arbitrary code.</p> <p>Debian: http://security.debian.org/pool/updates/main/r/remstats/</p> <p>There is no exploit code required.</p>	<p>Remstats Local Insecure Temporary File & Remote Code Execution</p> <p>CAN-2005-0387 CAN-2005-0388</p>	High	Debian Security Advisory, DSA 704-1, April 4, 2005
SCO Open Server 5.0.7	<p>A buffer overflow vulnerability has been reported in 'nwprint' due to insufficient bounds checking, which could let a malicious user obtain elevated privileges.</p> <p>No workaround or patch available at time of publishing.</p> <p>An exploit script has been published.</p>	SCO OpenServer NWPrint Command Buffer Overflow	Medium	Bugtraq, 394864, April 4, 2005
YepYep mtftpd .1a, 0.2, 0.3	<p>Two vulnerabilities have been reported: a format string vulnerability has been reported if the FTP server is compiled with the MT_DEBUG option (which is not the default configuration) because the 'log_do()' function in 'log.c' contains a syslog call without a format string specifier, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability has been reported in the 'mt_do_dir' function, which could let a remote malicious user execute arbitrary code.</p> <p>No workaround or patch available at time of publishing.</p> <p>Exploit scripts have been published.</p>	<p>YepYep MTFTPD Format String & Buffer Overflow</p> <p>CAN-2005-0958 CAN-2005-0959</p>	High	Securiteam, March 31, 2005

[\[back to top\]](#)

Multiple Operating Systems - Windows / UNIX / Linux / Other				
Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
AlstraSoft EPay Pro 2.0	<p>Several vulnerabilities have been reported: a vulnerability has been reported in 'index.php' due to insufficient verification of the 'view' parameter, which could let a remote malicious user execute arbitrary files; and a Cross-Site Scripting vulnerability has been reported in 'index.php' due to insufficient sanitization of the 'payment' and 'send' parameters, which could let a remote malicious user execute arbitrary HTML and script code.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, Proofs of Concept exploits have been published.</p>	<p>AlstraSoft EPay Pro Remote File Include & Cross-Site Scripting</p> <p>CAN-2005-0980 CAN-2005-0981</p>	High	Dcrab 's Security Advisory, April 2, 2005
Bay Technical Associates RPC3 Telnet F 3.05	<p>A vulnerability has been reported in the telnet daemon which could let a remote malicious user bypass authentication.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required.</p>	<p>Bay Technical Associates RPC3 Telnet Daemon Authentication Bypass</p> <p>CAN-2005-0957</p>	Medium	Security Focus, 12955, April 1, 2005

Cisco Systems Cisco VPN 3000 Concentrator, VPN 3002 Hardware Client 3.x, 4.x	A remote Denial of Service vulnerability has been reported due to an unspecified error in the SSL handling. Update available at: http://www.cisco.com/warp/public/707/cisco-sa-20050330-vpn3k.shtml Currently we are not aware of any exploits for this vulnerability.	Cisco VPN 3000 Concentrator Remote Denial of Service CAN-2005-0943	Low	Cisco Security Advisory, 64347, March 30, 2005
Cisco Systems IOS 12.2 ZA, SY, SXB, SXA, (17a) SXA, (14)ZA2, (14)ZA, (14)SY	A remote Denial of Service vulnerability exists when processing Internet Key Exchange (IKE) packets. Revision 1.2: Updated the 12.2(14)SY03 Release Notes URL in the Software Fixes and Versions section. Revision 2.0: Updated the advisory to reflect devices without the VPNSM may be affected. Added 12.2(17d)SX as an affected release train. Added information for determining the presence of the crypto feature set. Updates available at: http://www.cisco.com/warp/public/707/cisco-sa-20040408-vpnsn.shtml Currently we are not aware of any exploits for this vulnerability.	Cisco IOS Malformed IKE Packet Remote Denial of Service	Low	Cisco Security Advisory 50430, April 8, 2004 Cisco Security Advisory 50430 Rev. 1.2, January 5, 2005 Cisco Security Advisory 50430 Rev. 2.0, March 30, 2005
Early Impact ProductCart 2.7	Multiple input validation vulnerabilities have been reported: a Cross-Site Scripting vulnerability has been reported in the 'NewCust.asp,' 'storelocator_submit.asp,' 'techErr.asp,' and the 'advSearch_h.asp' scripts due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; and SQL injection vulnerabilities have been reported in the 'advSearch_h.asp,' and 'tarinasworld_butterflyjournal.asp' scripts, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	Early Impact ProductCart Multiple Input Validation	High	Security Focus, 12990, April 4, 2005
Francisco Burzi PHP-Nuke 6.0, 6.5, RC1-RC3, 6.5 FINAL, BETA 1, 6.6, 6.7, 6.9, 7.0 FINAL, 7.0-7.3, 7.6	Multiple Cross-Site Scripting vulnerabilities have been reported in various modules including the 'Search,' 'FAQ,' and 'Encyclopedia,' modules and the 'banners.php' script, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	PHPNuke Multiple Module Cross-Site Scripting	High	SecurityReason-2005-SRA#04, April 3, 2005
Horde Project Horde 3.0.4 -RC 2	A Cross-Site Scripting vulnerability has been reported due to insufficient validation of the page title in a parent frame window, which could let a remote malicious user execute arbitrary HTML and script code. Update available at: http://ftp.horde.org/pub/horde/horde-latest.tar.gz There is no exploit code required.	Horde Application Page Title Cross-Site Scripting CAN-2005-0961	High	Secunia Advisory: SA14730, March 29, 2005
InterAKT Online MX Kart 1.1.2, MX Shop 1.1.1	Multiple SQL injection vulnerabilities have been reported in 'index.php' due to insufficient sanitization of various id parameters, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	InterAKT Online MX Kart Multiple SQL Injection CAN-2005-0955 CAN-2005-0956	High	Secunia Advisory: SA14793, April 1, 2005
Lighthouse Development Squirrelcart	A vulnerability has been reported in 'index.php' due to insufficient sanitization of the 'crn' and 'rn' parameters, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	Lighthouse Development Squirrelcart SQL Injection CAN-2005-0962	High	Dcrab 's Security Advisory, March 30, 2005
Logics Software LOG-FT	A vulnerability has been reported due to an access validation error, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Logics Software LOG-FT Information Disclosure	Medium	Bugtraq, 394969, April 5, 2005

LucasArts Star Wars Jedi Knight: Jedi Academy 1.0.11	<p>A buffer overflow vulnerability has been reported in the 'G_Printf()' function, which could let a remote malicious user execute arbitrary code.</p> <p>No workaround or patch available at time of publishing.</p> <p>An exploit script has been published.</p>	Star Wars Jedi Knight: Jedi Academy Buffer Overflow CAN-2005-0984	High	Secunia Advisory, SA14809, April 4, 2005
Mozilla.org Mozilla Browser 1.7.6, Firefox 1.0.1, 1.0.2; K-Meleon K-Meleon 0.9; Netscape 7.2	<p>A vulnerability has been reported in the javascript implementation due to improper parsing of lambda list regular expressions, which could a remote malicious user obtain sensitive information.</p> <p>The vendor has issued a fix, available via CVS.</p> <p>There is no exploit code required; however, a Proof of Concept exploit has been published.</p>	Mozilla Suite/Firefox JavaScript Lambda Information Disclosure	Medium	Security Tracker Alert, 1013635, April 4, 2005
Mozilla.org Mozilla Browser Suite prior to 1.7.6 ; Thunderbird prior to 1.0.2 ; Firefox prior to 1.0.2	<p>A buffer overflow vulnerability has been reported due to a boundary error in the GIF image processing of Netscape extension 2 blocks, which could let a remote malicious user execute arbitrary code.</p> <p>Mozilla Browser Suite: http://www.mozilla.org/products/mozilla1.x/</p> <p>Thunderbird: http://download.mozilla.org/?product=thunderbird-1.0.2&os=win(=en-US</p> <p>Firefox: http://www.mozilla.org/products/firefox/</p> <p>Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/</p> <p>Gentoo: http://security.gentoo.org/glsa/</p> <p>Slackware: http://slackware.com/security/viewer.php?l=slackware-security&y=2005&m=slackware-security.000123</p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	Mozilla Suite/ Firefox/ Thunderbird GIF Image Processing Remote Buffer Overflow CAN-2005-0399	High	Mozilla Foundation Security Advisory 2005-30, March 23, 2005 US-CERT VU#557948
Multiple Vendors Activision Call of Duty 1.4, 1.5 b, Call of Duty United Offensive 1.5.1 b, 1.41, Return to Castle Wolfenstein 1.0, 1.1, Wolfenstein: Enemy Territory 1.0.2, 2.56; id Software Quake 3 Arena 1.1.7, 1.16 n, 1.31, Quake 3 Arena Server 1.29 g, 1.29 f; LucasArts Star Wars Jedi Knight II: Jedi Outcast 1.0.4, Star Wars Jedi Knight: Jedi Academy 1.0.11; Raven Software Soldier Of Fortune 2 1.0 3, 1.0 2	<p>A remote Denial of Service vulnerability has been reported when a malicious user submits a long message that is not properly truncated.</p> <p>Wolfenstein: Enemy Territory version 2.60 is not vulnerable.</p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	Quake 3 Engine Message Denial of Service CAN-2005-0983	Low	Securiteam, April 5, 2005
Multiple Vendors ALT Linux Compact 2.3, Junior 2.3; Apple Mac OS X 10.0-10.0.4, 10.1-10.1.5, 10.2-10.2.8, 10.3-10.3.8, Mac OS X Server 10.0, 10.1-10.1.5, 10.2-10.2.8, 10.3-10.3.8; MIT Kerberos 5 1.0, 5 1.0.6, 5 1.0.8, 51.1-5 1.4; Netkit Linux Netkit 0.9-0.12, 0.14-0.17,	<p>Two buffer overflow vulnerabilities have been reported in Telnet: a buffer overflow vulnerability has been reported in the 'slc_add_reply()' function when a large number of specially crafted LINEMODE Set Local Character (SLC) commands is submitted, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability has been reported in the 'env_opt_add()' function, which could let a remote malicious user execute arbitrary code.</p> <p>ALTLinux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html</p>	Telnet Client 'slc_add_reply()' & 'env_opt_add()' Buffer Overflows CAN-2005-0468 CAN-2005-0469	High	<p>iDEFENSE Security Advisory, March 28, 2005 US-CERT VU#291924</p> <p>Mandrakelinux Security Update Advisory, MDKSA-2005:061, March 30, 2005</p> <p>Gentoo Linux Security Advisories, GLSA 200503-36 & GLSA 200504-01, March 31</p>

<p>0.17.17; Openwall GNU*/Linux (Owl)-current, 1.0, 1.1; FreeBSD 4.10-PRERELEASE, 2.0, 4.0 .x, -RELENG, alpha, 4.0, 4.1, 4.1.1 -STABLE, -RELEASE, 4.1.1, 4.2, -STABLEpre122300, -STABLEpre050201, 4.2 -STABLE, -RELEASE, 4.2, 4.3 -STABLE, -RELENG, 4.3 -RELEASE-p38, 4.3 -RELEASE, 4.3, 4.4 -STABLE, -RELENG, -RELEASE-p42, 4.4, 4.5 -STABLEpre2002-03-07, 4.5 -STABLE, -RELENG, 4.5 -RELEASE-p32, 4.5 -RELEASE, 4.5, 4.6 -STABLE, -RELENG, 4.6 -RELEASE-p20, 4.6 -RELEASE, 4.6, 4.6.2, 4.7 -STABLE, 4.7 -RELENG, 4.7 -RELEASE-p17, 4.7 -RELEASE, 4.7, 4.8 -RELENG, 4.8 -RELEASE-p7, 4.8 -PRERELEASE, 4.8, 4.9 -RELENG, 4.9 -PRERELEASE, 4.9, 4.10 -RELENG, 4.10 -RELEASE, 4.10, 4.11 -STABLE, 5.0 -RELENG, 5.0, 5.1 -RELENG, 5.1 -RELEASE-p5, 5.1 -RELEASE, 5.1, 5.2 -RELENG, 5.2 -RELEASE, 5.2, 5.2.1 -RELEASE, 5.3 -STABLE, 5.3 -RELEASE, 5.3, 5.4 -PRERELEASE; SuSE Linux 7.0, sparc, ppc, i386, alpha, 7.1, x86, sparc, ppc, alpha, 7.2, i386</p>	<p>Apple: http://wsidecar.apple.com/cgi-bin/nph-reg3rdpty1.pl/product=05529&platform=osx&method=sa/SecUpd2005-003Pan.dmg</p> <p>Debian: http://security.debian.org/pool/updates/main/n/netkit-telnet/</p> <p>Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/</p> <p>FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:01/</p> <p>MIT Kerberos: http://web.mit.edu/kerberos/advisories/2005-001-patch1.4.txt</p> <p>Netkit: ftp://ftp.uk.linux.org/pub/linux/Networking/netkit/</p> <p>Openwall: http://www.openwall.com/Owl/CHANGES-current.shtml</p> <p>RedHat: http://rhn.redhat.com/errata/RHSA-2005-327.html</p> <p>Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57755-1</p> <p>SUSE: ftp://ftp.SUSE.com/pub/SUSE</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/n/netkit-telnet/</p> <p>OpenBSD: http://www.openbsd.org/errata.html#telnet</p> <p>Mandrake: http://www.mandrakesecure.net/en/ftp.php</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200503-36.xml http://security.gentoo.org/glsa/glsa-200504-01.xml</p> <p>Debian: http://security.debian.org/pool/updates/main/k/krb5/</p> <p>Currently we are not aware of any exploits for these vulnerabilities.</p>		<p>& April 1, 2005</p> <p>Debian Security Advisory, DSA 703-1, April 1, 2005</p> <p>US-CERT VU#341908</p>
<p>MySQL AB</p> <p>MySQL 4.0.23, and 4.1.10 and prior</p>	<p>A vulnerability was reported in the CREATE FUNCTION command that could let an authenticated user gain mysql user privileges on the target system and permit the user to execute arbitrary code.</p> <p>A fixed version (4.0.24 and 4.1.10a) is available at: http://dev.mysql.com/downloads/index.html</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200503-19.xml</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/mysql-dfsg/</p> <p>Mandrake:</p>	<p>MySQL CREATE FUNCTION Remote Code Execution Vulnerability</p> <p>CAN-2005-0709</p>	<p>High</p> <p>Security Tracker Alert ID: 1013415, March 11, 2005</p> <p>Gentoo Linux Security Advisory, GLSA 200503-19, March 16, 2005</p> <p>Ubuntu Security Notice, USN-96-1 March 16, 2005</p> <p>Mandrakelinux Security Update Advisory, MDKSA-2005:060, March 21, 2005</p> <p>Trustix Secure Linux Security Advisory, TSL-2005-0009, March 21, 2005</p>

	http://www.mandrakesecure.net/en/ftp.php Trustix: http://http.trustix.org/pub/trustix/updates/ ALT Linux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html RedHat: http://rhn.redhat.com/errata/RHSA-2005-334.html SuSE: ftp://ftp.suse.com/pub/suse/ Conectiva: ftp://atualizacoes.conectiva.com.br/ A Proof of Concept exploit has been published.			SUSE Security Announcement, SUSE-SA:2005:019, March 24, 2005 RedHat Security Advisory, RHSA-2005:334-07, March 28, 2005 ALTLinux Security Advisory, March 29, 2005 Conectiva Linux Security Announcement, CLA-2005:946, April 4, 2005
MySQL AB MySQL 4.0.23, and 4.1.10 and prior	A vulnerability has been reported that could let local malicious users gain escalated privileges. This is because the "CREATE TEMPORARY TABLE" command can create insecure temporary files. The vulnerabilities have been fixed in version 4.0.24 (when available): http://dev.mysql.com/downloads/ Gentoo: http://security.gentoo.org/glsa/glsa-200503-19.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/mysql-dfsg/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Trustix: http://http.trustix.org/pub/trustix/updates/ ALT Linux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html RedHat: http://rhn.redhat.com/errata/RHSA-2005-334.html SuSE: ftp://ftp.suse.com/pub/suse/ Conectiva: ftp://atualizacoes.conectiva.com.br/ A Proof of Concept exploit has been published.	MySQL Escalated Privilege Vulnerabilities CAN-2005-0711	Medium	Secunia SA14547, March 11, 2005 Gentoo Linux Security Advisory, GLSA 200503-19, March 16, 2005 Ubuntu Security Notice, USN-96-1 March 16, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:060, March 21, 2005 SUSE Security Announcement, SUSE-SA:2005:019, March 24, 2005 Trustix Secure Linux Security Advisory, TSL-2005-0009, March 21, 2005 RedHat Security Advisory, RHSA-2005:334-07, March 28, 2005 ALTLinux Security Advisory, March 29, 2005 Conectiva Linux Security Announcement, CLA-2005:946, April 4, 2005
MySQL AB MySQL 4.0.23, and 4.1.10 and prior	An input validation vulnerability was reported in udf_init() that could let an authenticated user with certain privileges execute arbitrary library functions on the target system. The udf_init() function in 'sql_udf.cc' does not properly validate directory names. A fixed version (4.0.24 and 4.1.10a) is available at: http://dev.mysql.com/downloads/index.html Gentoo: http://security.gentoo.org/glsa/glsa-200503-19.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/mysql-dfsg/ Mandrake: http://www.mandrakesecure.net/en/ftp.php	MySQL udf_init() Path Validation Vulnerability CAN-2005-0710	High	Security Tracker Alert ID: 1013414, March 11, 2005 Gentoo Linux Security Advisory, GLSA 200503-19, March 16, 2005 Ubuntu Security Notice, USN-96-1 March 16, 2005 SUSE Security Announcement, SUSE-SA:2005:019, March 24, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:060, March 21, 2005 Trustix Secure Linux Security Advisory, TSL-2005-0009, March 21, 2005

	<p>Trustix: http://http.trustix.org/pub/trustix/updates/</p> <p>ALT Linux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html</p> <p>RedHat: http://rhn.redhat.com/errata/RHSA-2005-334.html</p> <p>SuSE: ftp://ftp.suse.com/pub/suse/</p> <p>Conectiva: ftp://atualizacoes.conectiva.com.br/</p> <p>A Proof of Concept exploit has been published.</p>			<p>RedHat Security Advisory, RHSA-2005:334-07, March 28, 2005</p> <p>ALTLinux Security Advisory, March 29, 2005</p> <p>Conectiva Linux Security Announcement, CLA-2005:946, April 4, 2005</p>
<p>PHP Group</p> <p>PHP prior to 5.0.4</p>	<p>Multiple Denial of Service vulnerabilities have been reported in 'getimagesize().'</p> <p>Upgrade available at: http://ca.php.net/get/php-4.3.11.tar.gz/from/a/mirror</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/php4/</p> <p>Currently we are not aware of any exploits for these vulnerabilities.</p>	<p>PHP</p> <p>'getimagesize()' Multiple Denials of Service</p> <p>CAN-2005-0524 CAN-2005-0525</p>	<p>Low</p>	<p>iDEFENSE Security Advisory, March 31, 2005</p> <p>Ubuntu Security Notice, USN-105-1 April 05, 2005</p>
<p>ProfitCode Software</p> <p>PayProCart 3.0</p>	<p>Several vulnerabilities have been reported: a Directory Traversal vulnerability has been reported in the 'ftoedit' parameter, which could let a remote malicious user obtain sensitive information; and a Cross-Site Scripting vulnerability has been reported in the 'usrdetails.php' script due to insufficient validation of the 'sgnuptype' parameter, which could let a remote malicious user execute arbitrary HTML and script code.</p> <p>No workaround or patch available at time of publishing.</p> <p>Proofs of Concept exploit has been published.</p>	<p>ProfitCode Software PayProCart Directory Traversal & Cross-Site Scripting</p>	<p>Medium/ High</p> <p>(High if arbitrary code can be executed)</p>	<p>Dcrab 's Security Advisory, April 4, 2005</p>
<p>Samsung</p> <p>ADSL Modem</p>	<p>A vulnerability has been reported because common default accounts and passwords are used, which could let a remote malicious user obtain sensitive information.</p> <p>No workaround or patch available at time of publishing.</p> <p>Proofs of Concept exploits have been published.</p>	<p>Samsung ADSL Router Information Disclosure</p> <p>CAN-2005-0865</p>	<p>Medium</p>	<p>Security Tracker Alert, 1013615, March 31, 2005</p>
<p>SonicWALL</p> <p>SOHO 5.1.7 .0</p>	<p>Multiple input validation vulnerabilities have been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary code.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, Proofs of Concept exploits have been published.</p>	<p>SonicWALL SOHO Web Interface Multiple Remote Input Validation</p>	<p>High</p>	<p>Security Focus, 12984, April 4, 2005</p>
<p>Stalker Software, Inc.</p> <p>CommuniGate Pro 4.3 c2, 4.3 c1</p>	<p>A Denial of Service vulnerability has been reported when a malicious user submits multipart messages to a list.</p> <p>Upgrades available at: http://www.stalker.com/CommuniGatePro/default.html#Current</p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>CommuniGate Pro LIST Denial of Service</p>	<p>Low</p>	<p>Secunia Advisory, SA14604, April 5, 2005</p>
<p>Toshiba</p> <p>ACPI 1.60 BIOS; possibly 1.7 and 1.8</p>	<p>A Denial of Service vulnerability has been reported in the ACPI BIOS due to a coding error. <i>NOTE: it has been debated as to whether or not this issue poses a security vulnerability, since administrative privileges would be required, and other DoS attacks are possible with such privileges.</i></p> <p>No workaround or patch available at time of publishing.</p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>Toshiba ACPI BIOS Denial of Service</p> <p>CAN-2005-0963</p>	<p>Low</p>	<p>Portcullis Security Advisory, March 29, 2005</p>

[\[back to top\]](#)

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
April 5, 2005	x0n3-h4ck_MailEnable_Imapd.c	Yes	Script that exploits the MailEnable IMAP Authenticate Request Buffer Overflow vulnerability.
April 4, 2005	argo.c	No	Script that exploits the ArGoSoft FTP Server 'DELE' Command Remote Buffer Overflow vulnerability.
April 4, 2005	nwprintex.c	No	Script that exploits the SCO OpenServer NWPrint Command Buffer Overflow vulnerability.
April 2, 2005	codmsgboom.cfg	No	Script that exploits the Call of Duty / Call of Duty: United Offensive Denial of Service vulnerability.
April 2, 2005	jamsghof.cfg	No	Script that exploits the Star Wars Jedi Knight: Jedi Academy Buffer Overflow vulnerability.
April 1, 2005	101_netv.cpp 101_netvault.cpp	No	Exploit scripts for the BakBone NetVault Configure.CFG Local Buffer Overflow & Heap Overflow vulnerabilities.
April 1, 2005	snip-of-foo.WPA-profile-file snip-of-foo.RTO-profile-file	No	Proofs of Concept exploit scripts for the RUMBA Profile Handling Multiple Buffer Overflow Vulnerabilities.
March 31, 2005	0x666-ftpd.c mtftpd.c	No	Scripts that exploit the YepYep MTFTPD Remote Format String vulnerability.
March 30, 2005	897.cpp	No	Exploit for the phpBB versions 2.0.12 and below Change User Rights authentication bypass vulnerability.
March 30, 2005	Absinthe-1.3-Linux.tar.gz	N/A	A gui-based Linux version tool that automates the process of downloading the schema and contents of a database that is vulnerable to Blind SQL Injection.
March 30, 2005	Absinthe-1.3-MacOSX.tar.gz	N/A	A gui-based Mac OSX version tool that automates the process of downloading the schema and contents of a database that is vulnerable to Blind SQL Injection.
March 30, 2005	Absinthe-1.3-Windows.zip	N/A	A gui-based Windows version tool that automates the process of downloading the schema and contents of a database that is vulnerable to Blind SQL Injection.
March 30, 2005	n-lkernel2.6.10.c	Yes	Denial of Service exploit for Linux kernel versions 2.6.10 and below.
March 30, 2005	r57punbb.pl.txt	No	Exploit for the PunBB versions 1.2.2 and below authentication bypass vulnerability.
March 30, 2005	squirrelSQL.txt	No	Sample exploitation for the Lighthouse Development Squirrelcart SQL Injection vulnerability.
March 30, 2005	unrealmagic.c	Yes	Script that exploits the Cyrus IMAPD Multiple Remote Vulnerabilities.
March 29, 2005	AspApp.txt	No	Sample exploitation for the Multiple SQL injection and Cross-Site Scripting vulnerabilities.
March 29, 2005	portalApp.txt	No	Sample exploitation for the latek PortalApp SQL Injection and Cross-Site Scripting Vulnerabilities.

[back to top](#)

Trends

- **Pharming attacks against domain:** A warning was issued by the SANS Institute's Internet Storm Center (ISC) regarding new attacks that corrupt some Domain Name System (DNS) servers so that requests for .com sites sent to those servers connect users instead to Web sites maintained by the attackers. At 1,300 Internet domains were redirected to compromised Web servers in a similar attack in early March. Source: http://www.computerworld.com/securitytopics/security/hacking/story/0,10801,100813,00.html?source=NLT_PM&nid=100813.
- **ISPs, telecoms join to 'fingerprint' Internet attacks:** According to a statement published by a new group called the Fingerprint Sharing Alliance which is made up of leading global telecommunications companies, Internet service providers and network operators, they will begin sharing information on Internet attacks. The companies, including EarthLink Inc., Asia Netcom, British Telecommunications PLC and MCI Inc., will share detailed profile information on attacks launched against their networks. Source: <http://www.computerworld.com/printthis/2005/0,4814,100695,00.html>.
- **Internet aids access to sensitive identity data: Want someone else's Social Security number?** Social Security numbers are one of the most powerful pieces of personal information an identity thief can possess and are widely available and inexpensive despite public outcry and the threat of a congressional crackdown after breaches at large information brokers. Social Security numbers can be purchased for \$35 at www.secret-info.com, and \$45 at www.linforesearch.com, where users can also sign up for a report containing an individual's credit-card charges, as well as an e-mail with other "tips, secrets & spy info!" The Web site Gum-shoes.com promises that "if the information is out there, our licensed investigators can find it." Source: <http://www.washingtonpost.com/wp-dyn/articles/A23686-2005Apr3.html>
- **Hackers Write Spyware For Cash, Not Fame:** More than 70 percent of virus writers are now writing spyware under contract, one more piece of evidence that hacking has evolved from mischievous hobby to money-making criminal venture, a security firm reported Monday, April 4. Aladdin Knowledge Systems said its analysis showed that spyware is the favorite among malware writers, since it lets them re-wrap their own "technology" and sell it, or even introduce their own money-making ventures. Source: <http://www.techweb.com/wire/security/160403632>.
- **Sybase, NGSSoftware near agreement on publishing vulnerabilities:** Database maker Sybase will likely drop legal threats against a U.K.-based security company this week, allowing the company to publish details on six flaws, a source familiar with the negotiations said. Despite the probable resolution, attorneys and software-security experts warn that the recent legal attacks on vulnerability researchers could signal a resurgence of corporate interest in using the law to silence critical software reports. Source: <http://www.securityfocus.com/news/10821>.

[back to top](#)

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus identification reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trends	Date
1	Netsky-P	Win32 Worm	Stable	March 2004
2	Netsky-Q	Win32 Worm	Increase	March 2004
3	Zafi-D	Win32 Worm	Stable	December 2004
4	Bagle.BJ	Win32 Worm	Decrease	January 2005
5	Zafi-B	Win32 Worm	Stable	June 2004
6	Netsky-D	Win32 Worm	Stable	March 2004
7	Netsky-B	Win32 Worm	Slight Increase	February 2004
8	Netsky-Z	Win32 Worm	Slight Decrease	April 2004
9	Bagle-AU	Win32 Worm	Stable	October 2004
10	Sober-I	Win32 Worm	Return to Table	November 2004

Table Updated April 5, 2005

Viruses or Trojans Considered to be a High Level of Threat

- **Ahker-F:** Hackers have released this self-spreading worm that promises salacious movie clips of the celebrities. The e-mails contain text such as: "Watch Angelina Jolie and Brad Pitt cought (sic) on TAPE! SEXY CLIP! WATCH IT!" Source: http://news.com.com/Brad+Pitt+virus+targets+Microsoft/2100-7349_3-5648637.html?tag=cd.top
- **Chod.B:** A worm that first disguised itself as an e-mail from computer vendors is now attempting to trick MSN Messenger users into executing malicious files. The Chod.B worm, which was first discovered on April Fools' Day, spreads via e-mail purportedly from Microsoft and security companies Symantec and Trend Micro. Source: http://news.com.com/E-mail+worm+graduates+to+IM/2100-7349_3-5653697.html?tag=nefd.top
- **Mabir:** The Mabir worm, which targets Symbian Series 60 phones, is not spreading, but its ability to propagate via Multimedia Messaging Service messages (MMS) gives cause for concern. Instead of just reading all phone numbers from the local address book, Mabir-A replies with an infected MMS message in reply to any SMS or MMS messages sent to an infected phone. Source: http://www.theregister.co.uk/2005/04/04/mabir_mobile_worm/

The following table provides, in alphabetical order, a list of new viruses, variations of previously encountered viruses, and Trojans that have been discovered during the period covered by this bulletin. This information has been compiled from the following anti-virus vendors: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs, Panda Software, Computer Associates, and The WildList Organization International. Users should keep anti-virus software up to date and should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that anti-virus software detects.

NOTE: At times, viruses and Trojans may contain names or content that may be considered offensive.

Name	Aliases	Type
Backdoor.Fivsec		Trojan
Backdoor.Lateda.C		Trojan
BackDoor-CHC		Trojan
Beliu.A	Bck/Beliu.A	Trojan
Downloader-LG		Trojan
Downloader-MP		Trojan
Mabir.A	SymbOS/Mabir.A SymbOS.Mabir	Symbian OS Worm
Mydoom.BN	W32/Mydoom.BN.worm	Win32 Worm
Mytob.P	W32/Mytob.P.worm	Win32 Worm
Mytob.S	W32/Mytob.S.worm	Win32 Worm
Mytob.U	Net-Worm.Win32.Mytob.p W32/Mytob.U.worm	Win32 Worm
Mytob.V	Net-Worm.Win32.Mytob.r W32/Mytob.V.worm	Win32 Worm
Mytob.W	W32/Mytob.W.worm	Win32 Worm
PP97M.Xjan.dr		MS Powerpoint Virus
PWSteal.Lemir.H		Trojan
PWSteal.Reanet.C		Trojan
Skulls.G	SymbOS.Skulls.G SymbOS/Skulls.G	Symbian OS Worm
SymbOS.Skulls.H		Symbian OS Worm
SYMBOS_CABIR.E		Symbian OS Worm
Troj/Agent-CZ	Trojan-Proxy.Win32.Small.bh	Trojan

Troj/Bancos-BY	Trojan-Spy.Win32.Bancos.u PWS-Banker.gen.i trojan	Trojan
Troj/BankAsh-F	Trojan-Spy.Win32.Banker.mg PWS-Banker.j.dll	Trojan
Troj/Bdoor-ZAT		Trojan
Troj/PcClient-D		Trojan
Troj/StartPa-FM	Trojan.Win32.StartPage.sr Trojan.Startpage-220	Trojan
TROJ_ANICMOO.C	Exploit-ANIfile Trojan.Moo Win32.MS05-002!exploit	Trojan
TROJ_ASH.D	PWSteal.Bankash.E Troj/BankAsh-D Win32.Bankash.F	Trojan
Trojan.Ascetic.B		Trojan
Trojan.Littlog		Trojan
Trojan.Pim		Trojan
VBS.Haster@mm		Visual Basic Worm
VBS.Kuullio@mm	Email-Worm.BAT.Hobat.a	Visual Basic Worm
VBS.Ypsan.B@mm		Visual Basic Worm
W32.AllocUp.A		Win32 Worm
W32.Envid.O@mm	Email-Worm.Win32.Envid.e	Win32 Worm
W32.Kelvir.K		Win32 Worm
W32.Kelvir.M		Win32 Worm
W32.Mydoom.BI@mm		Win32 Worm
W32.Mytob.AA@mm		Win32 Worm
W32.Mytob.U@mm		Win32 Worm
W32.Serflog.C	W32/Crog.worm W32/Sumom-C Win32.Sumom.C Worm:Win32/Fatso.C WORM_FATSO.C	Win32 Worm
W32.Sory.A	Worm.Win32.Soriw	Win32 Worm
W32.Zori.B		Win32 Worm
W32/Ahker-F	WORM_AHKER.F Email-Worm.Win32.Anker.g	Win32 Worm
W32/Codbot-Gen		Win32 Worm
W32/Elitper-E	WORM_ELITPER.E	Win32 Worm
W32/Forbot-Gen		Win32 Worm
W32/Mytob-C		Win32 Worm
W32/Mytob-O		Win32 Worm
W32/Mytob-Q	WORM_MYTOB.Q	Win32 Worm
W32/Mytob-R	Net-Worm.Win32.Mytob.p Net-Worm.Win32.Mytob.q Worm.Mytob.H-3	Win32 Worm
W32/Rbot-APR	WORM_RBOT.APR Backdoor.Win32.Rbot.gen W32/Sdbot.worm.gen.g W32.Spybot.Worm	Win32 Worm
W32/Rbot-ZN	Backdoor.Win32.Rbot.gen	Win32 Worm
W32/Rbot-ZP		Win32 Worm
W32/Rbot-ZQ	Backdoor.Win32.Rbot.gen	Win32 Worm
W32/Sdbot-WN	Backdoor.Win32.IRCBot.ak W32/Sdbot.worm.gen.t	Win32 Worm
W32/Sdbot-WQ		Win32 Worm
W32/Sdbot-WS	Trojan.SdBot-447 W32/Sdbot.worm.gen.y	Win32 Worm
W32/Stubbot-A	Backdoor.Win32.Stub.b	Win32 Worm
Win32.Ahker.G		Win32 Worm
Win32.Bropia.W		Win32 Worm
Win32.Clspring Family		Win32 Worm
Win32.Inservice.T		Win32 Worm
Win32.Mytob.O		Win32 Worm
Win32.Mytob.S		Win32 Worm
Win32.Mytob.W	WORM_MYTOB.W	Win32 Worm

WORM_AHKER.F	Email-Worm.Win32.Anker.f Email-Worm.Win32.Anker.g W32.Ahker.F@mm W32/Ahker-F W32/Generic.m Win32.Ahker.G	Win32 Worm
WORM_CHOD.B	W32.Chod.B@mm Win32.NochoD.B	Win32 Worm
WORM_ELITPER.E	W32.Elitper.E@mm W32/Elitper-E W32/Generic.m Win32.Elitper.E Win32/Unknown!P2P!Worm Worm:Win32/Elitper.E	Win32 Worm
WORM_KELVIR.G	W32.Bropia W32/Kelvir.worm Win32.Bropia.W	Win32 Worm
WORM_MYDOOM.AI	W32.Mydoom.BI@mm W32/Mydoom	Win32 Worm
WORM_MYTOB.T	W32.Mytob.U@mm W32/Mytob-O W32/Mytob.gen@MM Win32.Mytob.U	Win32 Worm
WORM_MYTOB.V	Net-Worm.Win32.Mytob.c W32.Mytob.V@mm	Win32 Worm
WORM_MYTOB.X		Win32 Worm
WORM_MYTOB.Y		Win32 Worm
WORM_MYTOB.Z		Win32 Worm
WORM_SOBER.M		Win32 Worm
X97M.Grazz.A	Excel97Macro/Crazz.A IRC-Worm.MSExcel.Grazz X97M/Crazz.A X97M_CRAZZ.A	MS Excel Virus

[\[back to top\]](#)

Last updated April 06, 2005